4 Policy Considerations for Government

4.1 Policy development

4.1.1 As in any other area of government activity, to develop appropriate policy positions, governments must understand the environments which they seek to influence. The discussion of the e-commerce environment in chapter 2 and the scenarios drawn and potential countermeasures identified in chapter 3, provide a good foundation to consider the range of policy options available to government.

4.1.1 In formulating policy options, as noted previously, the RGEC has adopted two broad approaches. These are the “environmental” and the “tools and powers” approaches. The analysis in chapter 3 divides the possible countermeasures into these two groups.

4.1.2 From our analysis using these approaches, the RGEC has prepared the following recommendations for consideration by HOCOLEA and, in turn, government.

4.2 Recommendations

Environmental measures

The adoption of risk management strategies

4.2.1 Government should facilitate the development of e-commerce risk management strategies. This recommendation is analogous to the approach already taken by governments in relation to the physical environment: whereby the community is encouraged to be resistant to crime through environmental measures such as, security systems and, even, Neighbourhood Watch.

4.2.2 In many ways the task of raising awareness regarding the risks associated with e-commerce is very similar to the task facing government and industry several years ago in relation to the Year 2000 bug. Its potential impact on business was not understood by the community until a well orchestrated campaign was conducted by the Commonwealth Government, the Australian Stock Exchange (ASX) and industry organisations. As a result, most governments and companies, if not all, have Year 2000 programs in place to deal with the risks associated with this phenomenon. Consumers are far more aware of the need to ensure their goods and services are Year 2000 "compliant".

4.2.3 It is proposed that government work with:

- industry organisations such as the Australian Information Industry Association (AIIA), the Internet Industry Association (IIA), Australian Business Ltd, the Australian Industry Group, the State and Territory chambers of commerce and industry, the Australian Coalition of Service Industries, and others;
- Internet Service Providers;
- other organisations such as the ASX;
- insurance companies; and,
- consumer/user groups,

to put together an e-commerce risk management awareness campaign along the lines of the Year 2000 bug awareness and other consumer oriented programs.

4.2.4 The global coverage of the Internet introduces new issues, and consumers should be warned of the potential dangers of carrying out financial transactions – banking, purchasing, gambling, etc – with companies and organisations in jurisdictions where there is not the same consumer protection legislation as exists in Australia.

4.2.5 In all of the above awareness activity, care will need to be taken not to arouse undue or excessive concerns to the point of actually inhibiting the growth of e-commerce. This could be achieved through the preparation of easy-to-understand publications and good practice guidelines. For example, the Australian Computer Society has proposed an "Internet Driver's Licence". Programs such as this could assist in raising both awareness and competencies.

4.2.6 Components of a national risk management strategy could include IT skills development, the development of IT security response and intelligence capabilities, certificates and record keeping obligations for ISPs. As with risk management strategies in other environments, such a campaign could include awareness raising in respect of obligations to use Web site identifiers. Each of these is considered in turn.

4.2.7 This recommendation builds on existing government strategies in educating consumers. For example, NOIE and Treasury has produced materials, including 'Fact Sheets', advising consumers as to information they should identify on a Web site before engaging in e-commerce activities. In addition, the *Exposure Draft of the Policy Framework for Consumer Protection in Electronic Commerce* released by the Minister for Financial Services and Regulation, foreshadows the development of a Model Code for Consumer Protection in Electronic Commerce[54].

[54] Available at:
http://www.treasury.gov.au/publications/ConsumerProtectionInElectronicCommerce/index.asp

Skills development

4.2.8 An awareness campaign will be of little value if the professional skills necessary to ensure the effective implementation of risk management strategies are not available. There is currently a widespread and growing shortage of skills in Internet security.

4.2.9 The consequences of such a shortage of skills will be inadequately configured firewalls, poorly protected computer systems and weak implementations of security products that might otherwise provide good protection.

4.2.10 Australian government could address this issue proactively by a five point strategy which:

- defines the core competencies required to protect computer systems and minimise risk.
- identifies and endorse certificate courses in Internet security offered by commercial training companies. Such certificate courses have been growing in popularity in recent years. They are typically self-paced and relatively cheap, and provide suitable specialist qualifications for those without formal tertiary accreditation in IT. Through entities such as the Federal Government's Business Entry Point, SMEs, in particular, could be encouraged to ask their Internet contractors for evidence of such qualifications. This could be a part of the general risk management awareness campaign. These certificate courses could ramp up quickly to meet shorter term needs.
- encourages tertiary institutions to include at least one semester of Internet security in every vocational IT course. This would help to meet the longer term need.
- encourages the development of accreditation in Internet security by professional associations. Such associations might include the Information Systems Audit and Control Association (ISACA), the Australian Information Industry Association (AIIA) and the Australian Computer Society (ACS). Where the preceding steps would be aiming to make Internet security skill pervasive throughout the Australian IT industry, these professional associations would be focused more on the provision of more highly qualified specialists.

- ensures that the same probity checks which are undertaken in respect of physical security personnel are applied to e-commerce security personnel.

4.2.11 In the longer term, governments may seek to formally regulate Internet security specialists in the same way that state governments currently regulate the physical security industry. This should not take place until a proven need to do so emerges. It is noteworthy that the Australian IT industry is considered to be one of the best in the world. This opportunity should be embraced as one of our positioning strategies and the development of legitimate systems testing skills should therefore be proactively encouraged by Australian governments.

The development of IT security response and intelligence capabilities

4.2.12 To be able to combat Internet-based crime, it is essential that as many security breaches as possible be registered under an appropriate notification scheme.

4.2.13 If this is to occur, one of the issues to be determined is how this requirement should be met.

Use of Electronic Authentication

4.2.14 More widespread use of electronic authentication by Web servers would allow relying parties to have greater confidence in the identity and business bona fides of those operating Web servers. In both cases, the ensuing confidentiality would prevent possible fraud, theft of intellectual property and breaches of privacy. This can be achieved by government using and requiring electronic authentication in its business dealings.

4.2.15 The Australian Government should undertake a campaign to encourage the widespread use of electronic authentication by e-commerce participants.

4.2.16 Wider use of electronic authentication, especially for e-mail, would ensure that provable authorship of communications is widespread, facilitating investigations and, if necessary, prosecutions associated with Internet-related crimes. Benefits for business could include limitation of liability for fraud by employees or others.

Assessment of the adequacy of record keeping by Internet Service Providers

4.2.17 In the conventional environment, record keeping obligations are imposed on business for a number of purposes. Government must always consider the compliance burden created by such obligations, as well as the utility of those records to relevant authorities. Consideration should also be given to the privacy concerns of Internet users regarding access to and use of personal information.

4.2.18 As to whether, and for how long, ISPs should keep records including identity information is a matter for further consideration. The Internet is not yet at the stage where either appropriate retention periods or the frequency with which agencies would seek records, could be determined.

4.2.19 On-line tools can be used, in most circumstances, to identify the Internet Service Provider for an individual or organisation which is under investigation. If an ISP keeps records they will be likely to hold useful information about the person or company associated with the computer (or Web site) in question. If kept, this data could be accessed under warrant.

4.2.20 The challenge for both government and industry is to design a record keeping obligation which is both commercially sustainable and effective for its purpose.

4.2.21 An aid to the quest for a suitable arrangement would be the adoption of the risk management strategies referred to earlier. A record keeping obligation which leverages off commercial practices is not only desirable but essential if a workable system is to be found.

Web site identifiers

4.2.22 Commercial Web sites should display official identification information, i.e. an ABN or trading name. This would not only assist law enforcement and revenue agencies, but also assist consumers in identifying with whom they are dealing.

4.2.23 This recommendation is consistent with the OECD's draft Consumer Protection Guidelines for Electronic Commerce and with the advice provided to consumers via the NOIE 'Fact Sheets'.

Tools and powers

4.2.24 At this stage in the development of e-commerce, it is difficult to determine with any certainty the full range of tools, powers, and offences which will be required to ensure that law enforcement and revenue agencies have sufficient capability to detect, investigate and prosecute crime relating to e-commerce. However, there are a number of specific recommendations which can be made in this area. These relate to the establishment of a national computer forensics capability, new offence and warrant provisions, international agreements and Internet media monitoring. Each of these is considered in turn.

National Computer Forensics capability

4.2.25 Many of the countermeasures to crime which exploits the characteristics of the Internet call for law enforcement and revenue agencies to use sophisticated tracing and other tools. They also call for these tools to be used by well trained specialists who retain their skills and maintain contact with industry. This would be a significant ongoing expense for government. To ensure such an investment is used effectively and as widely as is needed Australian governments should address the provision of a central computer and Internet forensic capability, available to all Commonwealth, State and Territory jurisdictions to support the investigation of computer and Internet-related crime[55].

4.2.26 Such a national capability would conduct online quick response investigations using all of the tracing tools previously described in this Report. To some extent, several law enforcement agencies already have such a capability. The proposal is to build upon this and provide a basis for further development which will be necessary as e-commerce and its parasitic crime evolve.

[55] This measure was a recommendation of the ECTF. An examination of how such a capacity could be created will be the subject of an Issues Paper in the RGEC's Second Series of Issues Papers.

4.2.27 IT forensic skills are also required at the "coalface" of law enforcement, because crime scene and other on site investigation requires skilled officers who can access a computer, recover data for evidentiary purposes and determine its possible relevance to an investigation, without accidentally destroying evidence (with or without the help of software "boobytraps").

4.2.28 If this is to occur, one of the issues to be determined is how this requirement should be met.

New Offence and Investigation Provisions

4.2.29 There is a range of possible legal reforms which may be necessary to facilitate the investigation and prosecution of offences involving e-commerce.

4.2.30 Potential new offences in this area are considered in the Australasian Centre for Policing Research (formerly the NPRU) Paper, *Minimum provisions for the investigation of computer based offences*. The Model Criminal Code Officers Committee is also working on possible offence provisions.

4.2.31 It may be that amendments will be required to existing investigative powers, such as warrant provisions, so as to facilitate on-line investigations. It is important that investigators have sufficient powers to deal with the full range of serious offences that are likely to be committed in the course of e-commerce.

4.2.32 It is recommended that the necessary range of offences and investigative powers are identified and put in place.

International Agreements

4.2.33 International agreements should be put into place to ensure a high degree of cooperation in the detection, investigation and prosecution of electronic commerce related crimes which span more than one jurisdiction. These should take account of and be consistent with the consensus currently being developed in various international fora in relation to the law enforcement and revenue implications of emerging cyberspace technologies.

4.2.34 Such agreements would also need to be consistent with and supported in Australian law by appropriate changes to the regime of assistance to foreign law enforcement established by the *Mutual Assistance in Criminal Matters Act 1987*. Any such amendments would need to take due account of issues of privacy and responsibility and be consistent with the law governing investigation and prosecution of purely domestic e-commerce offences.

4.2.35 The speed with which international cyberspace transactions can be conducted will inevitably pose a particular challenge to the existing mutual assistance regime based on time-consuming consideration of requests by central offices and courts. In some instances, consideration may need to be given to the appropriateness of this type of control on exchange of information, leading either to modification of the regime or to exclusion from it of certain matters. In such considerations, issues of privacy and responsibility will still need to be adequately addressed.

4.2.36 Some examples of areas in which international agreements and supporting domestic laws could assist are:

- Tracing attacks on computer systems: Agencies will need to be able to obtain and provide "real time" assistance to track cross-jurisdictional attacks.
- Obtaining admissible evidence: Australian evidence laws could be reviewed to ensure there are no obstructions to Australian courts evidence which has been obtained overseas by appropriate procedures.
- Investigation support: Agencies need to be able to obtain assistance from foreign agencies to pursue audit trails and obtain other investigative information.
- Tax treaties: Australia should review its position in relation to signing the OECD's Mutual Agreement on Tax Administration Matters. This is in addition to the traditional international tax treaties.

Internet Media Monitoring

4.2.37 To enhance the e-commerce intelligence gathering capability of law enforcement and revenue agencies, an Internet media monitoring infrastructure could be developed to allow cost effective, targeted and timely monitoring of public areas of the Internet.

4.2.38 Modern indexing and search techniques could be used to sift automatically through a large amount of material to find public activity of potential interest.

4.2.39 By monitoring public Internet media, such as newsgroups, mailing lists and web fora, just as it currently monitors print and conventional broadcast media, law enforcement and revenue agencies can become aware of possibly irregular activity as early as possible[56].

4.3 Conclusion

4.3.1 This Report has assessed the technical possibilities in relation to the maintenance of law enforcement and revenue agency capabilities in the electronic commerce environment and the wider information economy. It has also sought to provide a link between those technical possibilities and the various policy options governments may consider. In doing so, it recommends a range of strategies to be developed by government in consultation with business, industry and consumer groups.

4.3.2 The recommendations contained in this Report seek to address the role that the information economy's environment can play in assisting good governance as well as identifying specific measures which government may take to enhance law enforcement and revenue agencies' ability to contribute towards a safe and secure electronic commerce environment.

[56] The total amount of public material to be scanned for such targeted monitoring amounts to some 50 or so Gigabytes per day worldwide. This area is one where considerable efficiencies may be obtained by law enforcement and revenue agencies building a common facility.

Bibliography

Anderson, R. and F.A.P. Petitcolas. (1998). *On The Limits of Steganography, IEEE Journal of Selected Areas in Communication*, Volume 16, No. 4, Special Issue on Copyright and Privacy Protection.
Available at http://www.cl.cam.ac.uk/~fapp2/papers/jsac98-limsteg/.

Association of Australian Commercial Internet Providers submission to the Australian Broadcasting Authority On-Line Services Investigation, 1996.

Australian Bureau of Statistics. (1996). *1993-94 Business Use of Information Technology*, Australian Government Publishing Service, Canberra.

Australian Bureau of Statistics. (1997). *Household Use of Information Technology*. Australian Government Publishing Service, Canberra.

Australian Bureau of Statistics. (1997). *Computing Services Industry*, Australian Government Publishing Service, Canberra.

Australian Bureau of Statistics. (1998). *ABS Survey: Use of Internet by Householders, Australia*. August 1998 (Cat. No. 8147.0).

Australian Taxation Office. (1997). *Tax and the Internet*, Volume 1: Discussion report of the Australian Taxation Office Electronic Commerce Project Team on the challenges of electronic commerce for tax administration.

Bar-Hillel, M., D. Bar-Natan and B. McKay. (1998). "The Torah Codes: Puzzle and Solution". *Chance*, Volume 2, No. 2.
Available at http://cs.anu.edu.au/~bdm/dilugim/Chance.ps.

Barlow, J.P. (1995). 'Coming into the country', in Johnson D. Gl, and Nissenbaum H., Eds., 1995, *Computers*, *Ethics & Social Values*, Prentice Hall: Englewood Cliffs, NJ.

Balsamo, W & Carpozi, G. (1988). *Under the Clock: The Inside Story on the Mafia's First Hundred Years*, New Horizon Press. London.

Bank for International Settlements. (1996). *Implications for Central Banks of the Development of Electronic Money*. Bank for International Settlements. Basle. October 1996

Berwick, D. (1996). *Strategies to improve coordination by Australasian law enforcement agencies in the investigation of the use of computers for criminal paedophile activity.* National Police Research Unit. Adelaide.

Berwick D. (1998). *A Model for the future delivery of the Computer Investigation Techniques (CIT) Program incorporating the National Computer Crime Network (NCCN).* National Police Research Unit Board of Control papers. NPRU. Adelaide.

Biddle, C. B. (1996). “Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure”, *San Diego Law Review*, Vol. 33.
Available at http://www.acusd.edu/~biddle/mp.html.

Biddle, C. B. (1997). “Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace”, *World Wide Web Journal*, Volume 2, Issue 3 (Summer 1997), O’Reilly and Associates.
Available at http://www.acusd.edu/~biddle/LMW.htm.

Blaze, M., J. Feigenbaum and J. Lacy. (1996). “Decentralized Trust Management (PolicyMaker)” AT&T Research.
Available at ftp://research.att.com/dist/mab/policymaker.ps.

Blaze, M., J. Feigenbaum and A. D. Keromytis. (1997). “The Keynote Trust Management System”, Internet Draft.
Available at http://search.ietf.org/internet-drafts/draft-angelos-spki-keynote-00.txt.

Branchaud, M. (1997). “A Survey of Public Key Infrastructures”.
Available at http://www.xcert.com/~marcnarc/PKI/thesis/.

Callas, J., L. Donnerhacke, H. Finney and R. Thaye. (1998). “OpenPGP Message Format”. RFC 2440, November 1998.

Camdessus, M. (1998). *Money Laundering: The importance of international counter measures.* Address to the Plenary Meeting of the Financial Action Task Force on Money Laundering, Paris, 10 February 1998.

Carothers, T. (1998). ‘The rule of law revival’. *Foreign Affairs*, 77(2): 95-106, March/April 1998.

Carter, D. L & Katz, A. J. (1996/97). 'Computer Crime & Security', *Security Journal*, No.7, 1996; *Computer Security Issues & Trends*, Computer Security Institute / FBI Computer Crime and Security Survey, 1996 & 1997.

Chaum, D. (1982). *Blind signatures for untraceable payments.* Advances in Cryptology - Crypto ’82, 1982.

Chaum, D. (1985). *Security without identification: Transaction systems to make big brother obsolete.* Communication of the ACM, 28(10), 1985.

Chaum, D. (1992). *Achieving electronic privacy.* Scientific American, August 1992.

Clark, T. (1998). *Staff Writer*. CNET News.com, October 28, 1998.

Clarke, R. Internet Crime Prevention. Available at http://www.anu.edu.au/people/Roger.Clarke/II/IcrimPrev.html.

Coalition of Service Industries. (1998). *The 1998 Australian Service Sector Review*, Coalition of Service Industries. Canberra.

Commonwealth Attorney-General (1998). *Electronic Commerce: Building the Legal Framework*, Report of the Electronic Commerce Expert Group to the Attorney General, March 1998.

Computer Security Institute's (CSI). (1996). *1996 Computer Crime and Security Survey.* Available at http://www.gocsi.com.

Cottrell, L. (1997). "Mixmaster and remailer attacks".
Available at http://www.obscura.com/~loki/remailer/remailer-essay.html.

CSIRO (1997). *The Internet Report.*
Available at http://www.cmis.csiro.au/projects+sectors/atorepor.pdf.

Diffie, W. and S. Landau. (1998). "Privacy on the Line: The Politics of Wiretapping and Encryption", MIT Press, 1998.

Draft Electronic Transactions Bill (1999).
Available from http://www.law.gov.au/publications/ecommerce/interim2.html.

Economist. (1997). 'The perils of electronic shopping'. 1 November 1997.

Economist. (1998). 'You are being tailed'. 27 June 1998.

ECTF. (1996). *Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board.*
Available at http://law.gov.au/aghome/commprot/olec/ectfcont.html.

Elkins, M. (1996). "MIME Security with Pretty Good Privacy (PGP)", RFC 2015, October 1996.

Ellison, C. (1996). "Generalized Certificates".
Available at http://www.clark.net/pub/cme/html/cert.html.

Ellison, C. (1997). "Certification Infrastructure Needs for Electronic Commerce and Personal Use", submission to NIST.
Available at http://www.clark.net/pub/cme/nist-7-24/.

European Commission Information Society Report. "Towards a European Framework for Digital Signatures and Encryption".
Available at http://www.ispo.cec.be/eif/policy/97503.html

Felson, M. (1998). *Crime in Everyday Life.* (Second Edi.) Pine Farge Press. Thousand Oaks. California.

Ford, W. and M. S. Baum. (1997). *Secure Electronic Commerce*, Prentice Hall PTR.

Fortier, S. (1995). 'Firewalls provide hot new sales and service opportunities', *Computer Technology Review*, 24-27, Fall/Winter 1995.

Fortune. (1998). 'The E-Corporation'. 7 December 1998.

Freeh, L. (1996). "The International Crime Problem", Statement before the United States House of Representatives, Committee on International Relations, Hearing on Russian Organised Crime, 30 April.

Grabosky, P.N., Smith, R. G., & Wright, P. (1996). 'Crime and telecommunications' , *Trends and Issues in Crime and Criminal Justice*, No. 59, Australian Institute of Criminology, Canberra.

Grabosky, P.N. & Smith, R.G. (1998). *Crime in the Digital age: Controlling Telecommunications and Cyberspace Illegalities,* Federation Press, Leichhardt NSW.

Gutmann, P. (1997). “How to recover private keys for Microsoft Internet Explorer, Internet Information Server, Outlook Express, and many others (or Where do your encryption keys want to go today?)”.
Available at http://www.cs.auckland.ac.nz/~pgut001/pubs/breakms.txt, 1997

Gutmann, P. (1998). “Cryptography and Data Security”
Available at http://www.cs.auckland.ac.nz/~pgut001/.

Humphry, R. (1998). ‘Case for more corporate freedom’, *Australian Financial Review*, 13 January 1998.

Hundley & Anderson. (1996). ‘Emerging Challenge’, *Security Journal*, No.7, 1996.

IDC Directions 98. (IDC market briefing).

Internet Law Bulletin. (1998). Volume 1, No. 2, February 1998.

Johnson, N. (1998). “Steganography Tools and Software”.
Available at http://www.jjtc.com/Security/stegtools.htm.

Johnson, N. (1998). “Steganography and Digital Watermarking Tool Table”.
Available at http://www.jjtc.com/Steganography/toolmatric.htm.

Joint Committee of Public Accounts and Audit, Internet Commerce – To buy or not to buy? June 1998.

Jurisic, A. & Menezes, A. (1997). Eliptic curves and cryptography: Strong signature algorithms, *Dr Dobbs Journal*, April.

Mackrell, P. (1996). ‘Emerging Issues in Global electronic Commerce, proceedings of the 1996 NPRU Conference ‘World Wide Web of Crime - who's controlling the traffic?’

Marriot, P.R. (1988). *The Development of Computer and Other White Collar Crime*. Australian Crime Prevention Council.

Maurer, U. (1996). “Modelling a Public-Key Infrastructure”, Proceedings of the 1996 European Symposium on Research in Computer Security (ESORICS ’96).
Available at http://www.inf.ethz.ch/personal/maurer/publications.html

McCrone, J. (1997). ‘Information technology: Introducing cyber detectives’, *Security Australia*. November.

Monkerud, D (1995). 'Computer Security & Computer Crime', *Uniforum Magazine*, December 1995.

NOIE. (1998). *A Strategic Framework for the Information Economy*.
Available at http://www.noie.gov.au.

OSCA. (1997). *The Future of Computer Crime*, OSCA Seminar Proceedings 1/97

OSCA. (1998). *The Likely Changes in Telecommunications Technologies Over the Next Five Years and Their Implications for Law Enforcement Telecommunications Interception Capabilities*. Draft Paper. Office of Strategic Crime Assessments, Attorney General’s Office.

Petitcolas, F. A. P., R. J. Anderson and M. Kuhn. (1998). “Attacks on copyright marking systems”, Second Workshop on Information Hiding.
Available at http://www.cl.cam.ac.uk/~fapp2/papers/ih98-attacks/.

Petitcolas, F. A. P., R. J. Anderson and M. Kuhn. (1999). “Information Hiding — A Survey”, IEEE, Special Issue on Protection of Multimedia Content. May 1999.
http://www.cl.cam.ac.uk/~fapp2/papers/ieee99-infohiding.pdf.

President William J Clinton, Vice President Albert Gore, Jr. (1997). *A Framework for Global Electronic Commerce*, Washington D.C, July 1997.
Available at http://www.whitehouse.com.

Privacy Committee of New South Wales. (1995). *Smart Cards: Big Brother’s little helpers*. Report No.66.

Report of the G10 Working Party on Electronic Money, April 1997.

Richardson, C, and White, P. *Electronic Commerce and the Australian Taxation System: An exploratory study of six industries.*
Available from http://www.ato.gov.au/ecp/latrobun.htm.

Rivest, R. (1998). “Chaffing and winnowing: Confidentiality without encryption” Version of 1 July 1998 available at http://theory.lcs.mit.edu/~rivest/chaffing.txt, July 1998.

Rubin, A. and M. Reiter. (1998). “Crowds: Anonymity for Web Transactions”.
Available at http://www.research.att.com/projects/crowds/papers/j8.ps.gz.

Schneier, B. (1996). *Applied Cryptography: Protocols, algorithms and source code in C*, 2nd edition, John Wiley and Sons, 1996.

Schneier, B. (1998). Security pitfalls in cryptography.
Available at http://www.counterpane.com/pitfalls.html.

Smith, R. G. (1998). *Paying the Price on the Internet: Funds Transfer Crime in Cyberspace.* Internet Crime Conference, Melbourne, 16-17 February 1998, Australian Institute of Criminology, Canberra.

Sterling, C. (1995). *Crime without Frontiers.* McGraw Hill. New York.

Tapscott, D (1996). *The Digital Economy*. McGraw Hill. New York.

Thompson, D. E. (1998). *Electronic Commerce & Crime – The Foundations for an Australian Law Enforcement Response.* Office of Strategic Crime Assessments. Canberra.

UN Commission on Crime & Criminal Justice, Manual on the Prevention and Control of Computer-related Crime, New York, 1995.

Wayner, P. (1996). *Disappearing Cryptography: Being and Nothingness on the Net*. Academic Press.

Wieszyk, M. (1998). Computer evidence search and seizure: Results of national surveys and interviews. A report for the National Police Research Unit. Adelaide.

Williams, D. (1999). *Copyright Piracy and Enforcement*. 31 March 1999. (Attorney General’s Department Media Release – 547)

Internet references

http://www.nepean.uws.edu.au/users/johnf/payTV.txt.

http://www.pacificaccess.com.au/sbi/sbi_reports/yellow15.pdf.

http://www.isoc.org/images/mapv15.gif.

http://www.research.att.com/~lorrie/pubs/tech4kids/

http://www.cmis.csiro.au/projects+sectors/blocking.pdf

http://www.news.com/News/Item/0,4,28054,00.html.

http://www.intertrust.com

http//:www.adna.asn.au

http://www.law.gov.au/home/commprot/olec/olec.htm

http://www.rightsxchange.com/

http://www.auscert.org.au/

http://www.cert.org/

http://www.first.org/

http://www.isi.edu/in-notes/iana/assignments/port-numbers.

http://info.internet.isi.edu/in-notes/rfc/files/rfc2196.txt

http://info.internet.isi.edu/in-notes/rfc/files/rfc2504.txt

http://nsi.org/Library/Compsec/orangebo.txt

http://www.itsec.gov.uk

http://www.fish.com/~zen/satan/satan.html

http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.html

http://www.nua.ie/surveys/

http://www.cmis.csiro.au/pubs.

http://www.mp3.com/.

http://www.amazon.com/.

http://www.law.gov.au/publications/ecommerce/interim2.html.

ftp://ftp.isi.edu/in-notes/rfc2459.txt.

http://www.verisign.com/.

http://203.9.218.13/reports/npki/npkiworkingpartyreport.html.

http://www.anonymizer.com/

http://yourcommand.com/privacy/children.htm

http://www.neotrace.com/.

http://www.ted.cmis.csiro.au/proj/VERS/.