Australian Government
Australian Institute of Criminology

Resource materials on technology-enabled crime

Gregor Urbas
Kim-Kwang Raymond Choo

Technical and Background Paper

No. 28

ISSN 1445-7261
ISBN 978 1 921185 70 0

Project no. 0074a

Published by the Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601
Tel: (02) 6260 9272
Fax: (02) 6260 9299
Email: front.desk@aic.gov.au
Website: http://www.aic.gov.au

Please note: minor revisions are occasionally made to publications after release. The online versions available on this website will always include any revisions.

Disclaimer: The views expressed do not necessarily represent the policies of the Australian Government or AHTCC.

Edited and typeset by the Australian Institute of Criminology

Resource materials on technology-enabled crime

Gregor Urbas
Kim-Kwang Raymond Choo

Technical and Background Paper

No. 28

Contents

Figures

Tables

Foreword and acknowledgements

These resource materials were prepared by research staff at the Australian Institute of Criminology (AIC), principally by Dr Gregor Urbas, senior Lecturer at the ANU College of Law at the Australian National University and former AIC Research Analyst, with additional research and editing by Dr Kim-Kwang Raymond Choo, AIC Research Analyst. The glossary of terms is based on work done by Dr Tony Krone, former AIC Research Analyst.

Earlier drafts were read and commented on by the following, although the AIC accepts responsibility for this final version.

- Members of the forensic computing sub-group of the Electronic Evidence Specialist Advisory Group at the National Institute of Forensic Science (NIFS): Jason Beckett (New South Wales Police), Gregory Sevior (Victoria Police), Melanie Johnston (Northern Territory Police), Barry Blundell (South Australia Police), Tim Thomas (Western Australia Police) and Paul Reedy (Australian Federal Police)
- Dr Tony Raymond, Director, National Institute of Forensic Science
- Mr Kevin Zuccato, former Director, and staff at the Australian High Tech Crime Centre (AHTCC)
- Dr Shane McKenzie (University of Melbourne)
- Dr Jonathan Clough (Monash University)
- Mr Nicholas Cowdery AM QC, Director of Public Prosecutions NSW
- Mr Rob McCusker, former Research Analyst, AIC
- Dr Russell G Smith, Principal Criminologist, AIC

The following attended and advised at the roundtable:

- Mr Richard Refshauge SC, Director of Public Prosecutions, ACT
- Mr Paul Westwood, Director, Forensic Document Services
- Mr Nicholas Adamo, Director, Forensic Data Services
- Mr Damian Bugg QC, Commonwealth Director of Public Prosecutions

Staff of the JV Barry Library at the AIC assisted in sourcing relevant literature.

1
Introduction

Background

In December 2005, the Australian Institute of Criminology (AIC) was commissioned by the Australian High Tech Crime Centre (AHTCC) to conduct research into issues relating to key criminal justice issues concerning technology-enabled crime in the context of an evolving international and domestic legal and law enforcement framework.

As part of this research, the present resource materials were prepared to provide a general overview of information on technology-enabled crime to assist prosecutors and members of the judiciary who may be faced with proceedings involving technology-enabled crime.

This document should not, however, be viewed as an authority on technology-enabled crime or related prosecutions. Work on technology-enabled crime is ongoing and is a relatively new field. This compendium aims to present prosecutors with common terms, concepts, relevant legislation, and current debates in the academic literature affecting technology-enabled crime cases. The work profiled in this report does not necessarily represent best practice by law enforcement or the judiciary. As yet the work in this area is still in its infancy and standards have yet to be fully defined. Efforts are underway to develop more standardised, nationally-endorsed practices for computer forensics but this task will take time to complete. In the short term, computer forensic processes and practice will continue to evolve, driven by new technologies and software, and the intent nationally and internationally to standardise evidentiary processes and the science behind practice. Such dynamism will continue to generate subsequent challenges for practitioners and the judiciary, and compound the risk that research results will become rapidly outdated. These changes have fuelled ongoing debate about the perceived role of, and demands on, computer forensics police teams and court experts, given increasing use of computers in modern policing and in criminal activities.

The field of computer forensics is likely to be highly dynamic in many ways. In Australia, there is a lack of critical mass in prosecutions, especially in denial of service (DoS) attacks, to develop the necessary case law required to establish benchmarks. The work presented in this report, however, provides a useful summary, offering a solid basis on which to build greater understanding of technology-enabled crime cases and prosecutions that will serve to strengthen future work and policy debate in this field.

Terminology and definitions

There is currently a lack of consistency in terminology in the literature on aspects of computer crime with the following adjectives having been used to describe various aspects of computer-related crime:

- virtual
- online
- cyber-
- digital
- high tech
- computer-related
- internet-related
- telecommunications-related
- computer-assisted
- electronic
- ICT-related
- e- (as in e-crime).

Clearly, there are different contexts in which each of these descriptive terms is more appropriate. For example, hacking into freestanding un-networked computer systems and databases preceded the advent of the internet in its current form, and so the terms internet crime or online crime are inappropriate to deal with these earlier forms of activity.

Even spelling and usage show variations, particularly with regard to the use of the prefix cyber. The literature contains references to *cybercrime*, *cyber crime* and *cyber-crime*, as well as more specific forms such as *cyberterrorism* (or *cyber-terrorism*), *cyberstalking* (or *cyber-stalking*) and so on. The same variability applies to terms such as *e-crime* (sometimes *E-crime* or *eCrime*) (see Smith, Grabosky & Urbas 2004: 5-6 for a discussion of this issue). Traditionally, a distinction was drawn between crimes in which information and communications technologies were the object or the *target* of offending, and crimes in which technologies were the *tool* in the commission of the offence.

This latter category incorporated two levels of reliance on technologies: offences which were *enabled* by technologies (i.e. in which a computer was required for the commission of the offence); and offences which were *enhanced* by technologies (i.e. in which computers made it easier to commit an offence).

- Examples of information and communications technologies which are the object or target of offending include: illegal access/hacking; illegal interception of communications; data interference/viruses; system interference, denial of service/spam; misuse of devices/theft of services fraud (phreaking); and terrorism-related offences.
- Examples of technology-enabled offending in which information and communications technologies are necessary to commit the offence include: manipulation of data to obtain a fraudulent payment; ATM fraud; using technologies to commit forgery; sharemarket manipulation; stealing intellectual property; cyberstalking; collection and dissemination of illicit online content, such as child pornography; and phishing.
- Examples of technology-enhanced offending in which information and communications technologies are used to support the commission of the offence include: recording payments for drugs; establishing databases of victims or potential victims; identity theft; extortion; communicating between offenders/conspiracies; and encrypting secret information or using steganography to hide data.

These resource materials focus on technology-enabled crimes which are, arguably, the types of offending which are most directly related to misuse of ICT for criminal purposes. Where some specific forms of technology-enabled crime are discussed, the materials will use terms such as *cybercrime*, *cyberstalking* and so on in conformity with Australian legislation such as the *Cybercrime Act 2001* (Cth) and international instruments such as the Council of Europe *Convention on Cybercrime*.

The focus is, however, on crimes that require ICT for their commission, rather than conventional crimes which may, incidentally have ICT involved in some way. To assist readers of these resource materials in understanding some of the technical jargon, a detailed glossary of key terms is included at the end of the report.

Brief historical background

Telecommunications technologies were first created in 1837, and criminal misuse occurred as early as 1867 when an instance of illegal interception occurred (see Grabosky & Smith 1998). The 1960s saw a rapid expansion in the use of telephony services which corresponded with attempts to obtain services for free through ‘phreaking’ (which involved the use of devices such as whistles to simulate the frequency of a signal used by automated telephone systems to permit telephone services to be obtained dishonestly for free). The introduction of electronic funds transfer technologies such as ATM and EFTPOS led to the use of such facilities to transfer funds illegally in the 1970s. This was followed by the widespread use of computer networks which corresponded with the commission of money laundering and hacking offences. The introduction of the internet in the late 1980s created an environment in which copyright could be infringed and offensive materials disseminated across international networks. Wireless technologies of the 21st century have created new opportunities for misuse.

The last three decades of the 20th century produced numerous hacker groups devoted to finding ways of gaining unauthorised access to both freestanding computers and networked systems (HTCB no. 5, no. 6 and no. 7). The activities of these groups started to attract serious attention from law enforcement agencies when they succeeded in hacking into defence, government and university computers and altering data or leaving messages boasting of their exploits. The increasing use of computer records for storing information also provided opportunities for criminal exploitation of personal and financial information, facilitating new forms of fraud, extortion and theft.

The internet has also facilitated an explosion in the distribution of offensive or illegal content such as online child pornography. This has led increasingly to large scale international law enforcement operations directed at those responsible (HTCB no. 2 and no. 8; Forde & Patterson 1998; Grant, David & Grabosky 1997; Krone 2005a).

Grabosky & Smith (1998: 14–17) identified the following among the types of telecommunications-related crime emerging in the digital age:

- illegal interception of telecommunications
- electronic vandalism and terrorism
- stealing communications services
- telecommunications piracy
- pornography and other offensive content
- telemarketing fraud
- electronic funds transfer crime
- electronic money laundering.

These categories can be seen to comprise two overlapping domains. The first includes illegal activities directed at, or perpetrated through, the use of *computers*. This can involve: theft of computers; wilful damage to computers or computer systems; unlawful access to, or interference with, the operations of computers; transmitting offensive or illegal content using computers; and committing fraud or other offences through the use of computers. In turn, it is possible to distinguish between computers and ICT as the object of offending, and computers and ICT as a tool for offending (HTCB no. 1). This area of criminality is naturally most amenable to regulation through laws specifically directed at computer use and misuse, such as the computer offences contained in the *Criminal Code Act 1995* (Cth) and other legislation discussed below.

A wider but related area is the protection of *information*, which in the digital age increasingly means the protection of computer data and networks supporting the communication of information such as telecommunications systems. Protection of information has been a concern of legal systems from well before the introduction of modern technologies of mass communication, but is brought into sharp focus by the development of global computer-based information networks such as the internet. Principal legal measures related to the protection of information from unlawful use, distribution or exploitation include intellectual property laws, privacy laws, laws relating to secrecy and national security, telecommunications laws, and laws relating to unfair commercial advantage.

A useful analysis of the historical development of computer-related law is provided by Sieber (1998), who identified six waves of computer-related legislation beginning in the 1970s:

- privacy protection laws (e.g. relating to data held in government computers)
- economic crime laws (e.g. computer fraud)
- intellectual property laws (e.g. copyright and patent protection for computers and software, database protections)
- illegal and harmful content laws (e.g. electronically distributed pornography and racist propaganda)
- criminal procedural laws (e.g. relating to search and seizure of computers)
- security law (e.g. use of access controls such as encryption to protect data).

More recent attention on security issues in the context of terrorist threats and the protection of critical infrastructure has, of course, given new impetus to the development of security laws including significantly expanded law enforcement powers with respect to computers and telecommunications.

Main types of technology-enabled crime

The range of technology-enabled crime is always evolving, both as a function of technological change and in terms of social interaction with new technologies. Broadly speaking, such crimes can be categorised (Smith, Grabosky & Urbas 2004) according to whether they are:

- directed at computers and associated technologies such as computer intrusions (e.g. hacking and unauthorised access), denial of service (DoS) attacks, distributed denial of service (DDoS) attacks using botnets, cryptovirology/denial of resource attacks (e.g. the use of ransomware), the creation and distribution of malware (e.g. viruses, worms, Trojans and rootkits), and sabotage
- using computers and associated technologies (e.g. online child exploitation, cyberstalking, extortion, fraud and identity theft)
- with ancillary uses of computers and associated technologies such as internet markets for illicit goods and services, acquisition of high tech crime tools (HTCB no. 11 and no. 12), criminal uses of encryption or steganography to conceal activities and evidence.

Some criminal activities have emerged rapidly within recent times. For example, while phishing was unheard of just a few years ago, the public is now largely aware of the risks of answering unsolicited emails from senders purporting to be banks and other entities seeking confirmation of financial details. This is an example of a crime type that uses technology and exploitation of human behaviour to succeed (HTCB no. 9). Related activities include SMiShing (dissemination of phishing messages using short message services (SMS) on mobile phones) and vishing (dissemination of phishing messages using voice over internet protocols, or VoIP).

High-tech criminals rely increasingly on malicious code (also known as malware) such as viruses, worms, Trojan horses or rootkit programs to overcome security protections on computers or networks, and to harvest information such as passwords and financial details to facilitate fraud or identity theft (HTCB no. 10 and no. 11). These crimes represent more sophisticated and multidimensional evolutions from previously largely discrete areas of offending such as hacking and computer fraud, and are often referred to as blended threats. This includes spy-phishing, a form of phishing attack, involving the use of various malicious applications, typically Trojan horses and spyware, to perpetrate online information theft (Choo, Smith & McCusker 2007).

Future trends

The discernible trends from past evolutions of technology-enabled crime that are likely to continue into the future include:

- increased dependence of individuals and organisations on computer-based technologies for storage and processing of information and communications
- correspondingly increased opportunities for misuse of these technologies by motivated individuals and criminal groups
- emergence of new protective technologies, services and behaviours in response to perceived threats
- exploitation of continuing technological vulnerabilities (syntactic attacks) and human vulnerabilities (semantic attacks) by criminals.

The interaction of these trends can be seen as somewhat cyclical. For example, widespread adoption of internet banking provided new opportunities for criminal exploitation through hacking, account hijacking, so-called man-in-the-middle phishing attacks, manipulation of data, and fraud directed at both financial institutions and customers. Increased protection of bank computer systems against intrusion or internal misuse and better auditing of transactions data generally shifted the focus of criminal activity towards identity theft and fraud, which requires access to personal and financial details of customers. This led to phishing attacks whereby consumers were tricked through bogus emails and fake websites into revealing identifying information and passwords. As the risks became more widely understood, criminal activity again shifted to the use of malware to surreptitiously capture and transmit these details without the user having to be tricked, which has in turn led to an increased focus on technological protections such as firewalls, encryption and anti-virus and privacy software.

One clear trend in technological development and social adaptation is the rapid and widespread uptake of portable devices such as mobile phones, wireless laptops, palm pilots and storage devices (including USB devices), which has resulted in new forms of exploitation such as war driving, theft of devices both as objects and as repositories of valuable information (Urbas & Krone 2006b), eavesdropping and sniffing of VoIP calls, man-in-the-middle attacks, denial of service (DoS) attacks, call interruption and making free calls on VoIP networks built over wireless local area networks, and malware exploiting vulnerabilities in mobile phones (Choo, Smith & McCusker 2007).

Prevalence and costs of technology-enabled crime

There are few reliable statistics on the prevalence of technology-enabled crime, at least in relation to some categories. For example, while specific incidents of unauthorised access or data modification (hacking) are periodically reported, there is no practical way of assessing how much of this type of activity occurs in general, in part because a significant proportion of incidents will not be reported, properly identified or even detected by victims. Similarly, while there are some quantitative estimates of the number of computers affected by particular viruses or other malicious programs that circulate through the internet, it is difficult to express this as a large number of discrete crimes committed by an individual offender, as opposed to a single crime with multiple victims.

Nonetheless, some indication of the prevalence of technology-enabled crime is given by surveys of industry groups and households. Based on a relatively small number of public and private organisations, the annual Australia's National Commputer Emergency Response Team (AusCERT) survey of public and private sector organisations in Australia indicated that:

- 42 percent of survey respondents in 2003 reported having experienced one or more electronic attacks in the previous 12-month period

- 49% reported one or more electronic attacks in the 2004 survey
- 35% reported one or more electronic attacks in the 2005 survey
- 22% reported one or more electronic attacks in the 2006 survey (AusCERT 2006).

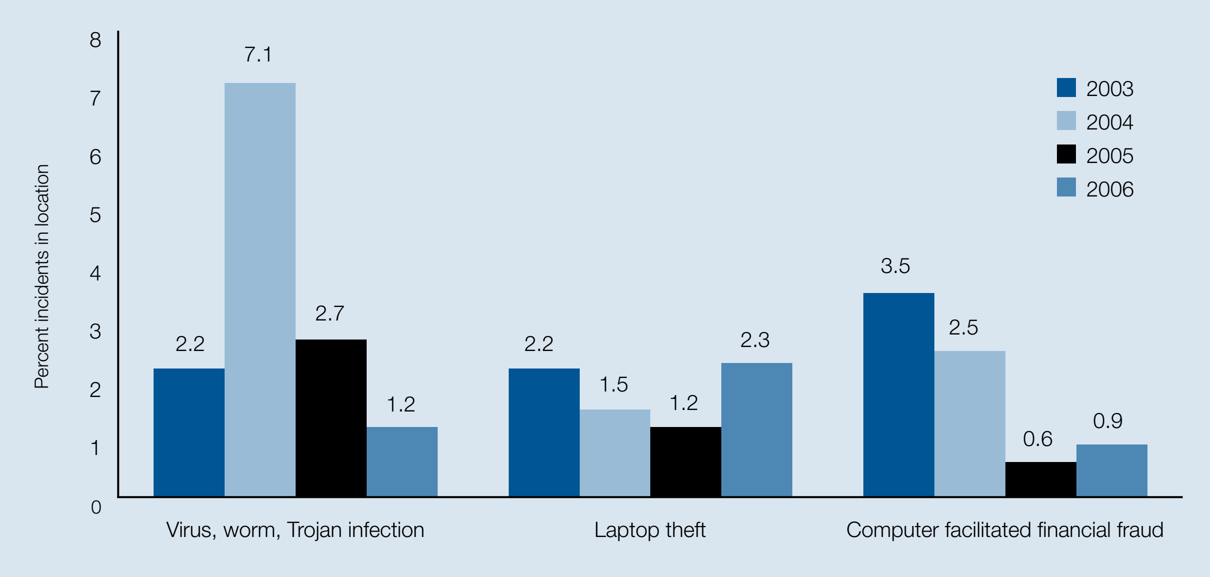
The Federal Bureau of Investigation (FBI) reported that financial loss due to cybercrime in 2004 was estimated to have been US$400 billion (McAfee 2005). A more recent survey in the United Kingdom (PWC 2006) also indicated that information security breaches cost United Kingdom companies across several industry sectors £10 billion per annum.

The most widely reported types of electronic attack or other computer crime over the same time periods have been:

- insider abuse of internet access, email or computer resources (62% in 2006)
- laptop theft (58% in 2006)
- virus, worm or Trojan infection (broken down in 2006 into 45% reporting self-propagating infections such as viruses or worms, and 21% reporting non-self-propagating malware such as Trojan or rootkit infection).

Although in the AusCERT (2006) survey, infections from viruses and worms were the most common form of electronic attack reported, the financial loss attributed to laptop theft is higher than that attributed to infections from viruses and worms. The chart below shows the costs attributed to these three types of offences over the four years (CFI no. 134).

Figure 1: Financial losses from technology-enabled crime, 2003–2006 ($m)



2006: 389 respondents, 2005: 181 respondents, 2004: 240 respondents, 2003: 214 respondents

Source: AusCERT (2006: 26)

Computer-related offending directed at or affecting households shares some of the same features, but few general crime victimisation surveys provide detailed information about particular types of high-tech crime. The International Crime Victimisation Survey last conducted in 2004 in Australia included some questions about consumers' experiences of online purchasing. Some 11 percent of those who made online purchases, mostly by giving credit card information, reported problems (Johnson 2005; Krone & Johnson 2006) such as:

- goods/services not as advertised

- goods/services not delivered
- money taken from account at a time other than as agreed
- more money taken than authorised.

Not all of these reported problems necessarily involve criminal conduct. However, it can be concluded that a proportion of households using computers are affected by online fraud or other misconduct. Even if not directly victimised, this may cause other households to avoid using such services as online banking or purchasing for fear of being victimised.

Issues for law enforcement agencies, prosecutors and the courts

The Electronic Crime Strategy developed by the Australasian Police Commissioners in 2000 identified the following as key issues (particularly arising from the global nature of much high tech crime) for law enforcement:

- jurisdiction (whether jurisdiction exists and the problem of concurrent jurisdiction) – see section 'Jurisdictional, prosecution and sentencing issues'
- legislative difficulties brought about by differing criminal law regimes (e.g. requirement of dual criminality)
- managing strategic alliances and partnerships and ensuring security, confidentiality and flexibility of response (particularly in relation to the private sector)
- dealing with differing privacy regimes
- achieving mutual assistance in real time or close to real time
- heavy reliance on cooperation and assistance from telecommunications providers and internet service providers (ISPs)
- the transborder search of computer data banks and the interception of communications
- ensuring timely and strategic intelligence assessments
- managing and coordinating extraditions.

As investigations proceed towards prosecution, many of the same issues confront prosecution agencies. In addition, prosecutors face the following difficulties:

- clarifying elements of new offences and related evidentiary requirements
- presenting complex and technical evidence in court
- identifying and using appropriately qualified experts to undertake analysis or give evidence
- defence challenges to admissibility
- novel defences and defence arguments.

Courts hearing cases involving technology-enabled crimes, or other cases involving electronic evidence, face particular issues arising from:

- presentation of complex and technical evidence
- heavy reliance on expert opinion
- complex and novel arguments relating to admissibility of evidence or the exercise of discretions
- lack of comprehension of offence elements and evidence by jurors and lawyers
- novel defences and defence arguments (including in sentencing proceedings)
- imposing appropriate sentences on convicted offenders.

2
International developments and cooperation

International law enforcement response

It has been evident from early in the development of legal responses to technology-enabled crime that this type of activity easily crosses jurisdictional boundaries (Grabosky & Smith 1998; Grabosky, Smith & Dempsey 2001). Considerable attention has been paid therefore to the international dimensions of the law enforcement response, with a focus on three main areas:

- harmonisation of substantive computer offences in national legislation
- harmonisation of procedural provisions relating to investigation and prosecution of technology-enabled crimes
- establishment/enhancement of cooperative mechanisms allowing exchange of information, evidence and the extradition of suspects.

Each of these areas has been influenced by the activities of numerous international bodies and cooperative arrangements. The following are some of the more significant international developments in this regard.

Organisation for Economic Co-operation and Development

The Organisation for Economic Co-operation and Development (OECD) made an early contribution in a 1986 report entitled *Computer-related crime: analysis of legal policy*, which recommended that member states pay particular attention to the coverage under their national penal laws of specific knowingly committed acts:

- the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit an illegal transfer of funds or of another thing of value
- the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit a forgery
- the input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or of a telecommunication system
- the infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put it on the market
- access to or interception of a computer and/or telecommunication system made knowingly and without the authorisation of the person responsible for the system, either by infringement of security measures or for other dishonest or harmful intentions.

In 1992, the OECD published its *Guidelines on information security*, which were revised and republished in 2002 as *Guidelines for the security of information systems and networks: towards a culture of security*. These guidelines were developed with the following aims (OECD 2002):

- promote a culture of security among all participants as a means of protecting information systems and networks
- raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation
- foster greater confidence among all participants in information systems and networks and the way in which they are provided and used
- create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks

- promote cooperation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures
- promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

The OECD guidelines then set out principles for participants in the development of security of information systems (OECD 2002):

- awareness: participants should be aware of the need for security of information systems and networks and what they can do to enhance security
- responsibility: all participants are responsible for the security of information systems and networks
- response: participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents
- ethics: participants should respect the legitimate interests of others
- democracy: the security of information systems and networks should be compatible with essential values of a democratic society
- risk assessment: participants should conduct risk assessments
- security design and implementation: participants should incorporate security as an essential element of information systems and networks
- security management: participants should adopt a comprehensive approach to security management
- reassessment: participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

In 2005, the OECD added to this with a report on *The promotion of a culture of security for information systems and networks in OECD countries* (OECD 2005). This report highlighted the important security role of:

- e-government applications and services
- protection of national critical information infrastructures
- computer security response teams (CERTs)
- outreach to small and medium-sized enterprises (SMEs).

The approach advocated by the OECD has been followed in Australia with the creation of the Trusted Information Sharing Network (TISN) and the cooperative operations of the AHTCC.

G8 countries

The Group of Eight (G8) countries are Canada, France, Germany, Italy, Japan, Russia, the United States and the United Kingdom. In the mid-1990s, groups of experts were formed from G8 meetings to address particular aspects of transnational crime, including a Subgroup on High-Tech Crime which has worked on:

- creation of its Network for 24-Hour Points of Contact for High-Tech Crime, currently with 45 members (including the addition of six new members in 2005 (Republic of China 2006)), and an international critical information infrastructure protection directory
- negotiation of widely-accepted principles and an action plan to combat high tech crime, subsequently adopted by G8 justice and home affairs ministers, endorsed by G8 heads of state, and recognised by other international fora

- various better practices documents, including guides for security of computer networks, international requests for assistance, legislative drafting, and tracing networked communications across borders
- assessments of threats and impact to law enforcement from new wireless technologies, encryption, and viruses, worms and other malicious code
- training conferences for cybercrime agencies from every continent (except Antarctica)
- conferences for law enforcement and industry on improved cooperation and tracing criminal and terrorist communications, and for all stakeholders on protection of critical information infrastructures.

The G8 countries have recently also turned their attention to the threat of the convergence of cybercrime and terrorist activity:

> Computers and computer networks have increasingly become both the objects of terrorist and other criminal attacks, and the conduit through which terrorists and other criminals communicate to plan and carry out their destructive activities. Because many computer networks transcend international borders, it is essential that all countries have adequate substantive and procedural laws, and that they cooperate successfully to investigate, so as to prevent and punish terrorist and other criminal activities perpetuated with the aid of computers and computer networks …
>
> States should review their laws to ensure that abuses of modern technology that are deserving of criminal sanctions are adequately criminalized and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention, and international cooperation in respect of such abuses are effectively addressed (G8 2005).

In their 2005 recommendations, the G8 countries endorsed the *Convention on Cybercrime* (COE), and urged international efforts to combat the sexual exploitation of children on the internet (G8 2005).

United Nations

The United Nations (UN) has been monitoring developments in computer-related crime for over a decade, starting with the 8th United Nations Crime Congress in Havana in 1990. This was followed in 1994 by the publication of the *UN manual on the prevention and control of computer-related crime* (UN 1994).

A UN symposium, The challenge of borderless cybercrime, was held in conjunction with the Palermo signing conference of the *Convention Against Transnational Organized Crime* in December 2000 (UN 2000). The Vienna Declaration on Crime and Justice: *Meeting the challenges of the 21st century*, was adopted by the 10th UN Congress on the Prevention of Crime and the Treatment of Offenders in April 2000 (UN 2001). This declaration included a commitment:

> … to develop action-oriented policy recommendations on the prevention and control of computer-related crime, and … working towards enhancing our ability to prevent, investigate and prosecute high-technology and computer-related crime.

The connections between organised crime, particularly in the form of terrorism, and cybercrime continued as a focus of the 11th UN Crime Congress in 2005. This meeting recognised that:

> … besides traditional threats to peace and security, new dangerous threats had emerged on a global scale which were interconnected and should no longer be seen in isolation from one another, in particular threats related to transnational organized crime, including drug trafficking, but also to corruption and terrorism.

In this context, cybercrime and money laundering were described as emerging concerns (UN 2005). A UN Working Group on Internet Governance was established to contribute to the World Summit on the Information Society which was held in Tunisia in November 2005.

Council of Europe

In 1989, the Select Committee of Experts on Computer-Related Crime of the Council of Europe (COE) produced a minimum list of computer crimes to be prohibited and prosecuted by international consensus (Goodman & Brenner 2002: note 172):

- computer fraud: The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person
- computer forgery: the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence
- damage to computer data or computer programs: the erasure, damaging, deterioration or suppression of computer data or computer programs without right
- computer sabotage: the input, alteration, erasure or suppression of computer data or computer programs, or other interference with computer systems, with intent to hinder the functioning of a computer or a telecommunication system
- *unauthorised access*: the access without right to a computer system or network by infringing security measures
- unauthorised interception: the interception, made without right and by technical means, of communications to, from and within a computer system or network
- unauthorised reproduction of a protected computer program: the reproduction, distribution or communication to the public without right of a computer program which is protected by law
- unauthorised reproduction of a topography: The reproduction without right of a topography protected by law, of a semi-conductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semi-conductor product manufactured by using the topography.

The COE committee also provided an optional list on which it would be harder to reach international consensus (Goodman & Brenner 2002: note 173):

- alteration of computer data or computer programs: the alteration of computer data or computer programs without right
- computer espionage: the acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person
- unauthorised use of a computer: the use of a computer system or network without right, that either: (a) is made with the acceptance of a significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning; or (b) is made with intent to cause loss to the person entitled to use the system or harm to the system or its functioning; or (c) causes loss to the person entitled to use the system or harm to the system or its functioning
- unauthorised use of a protected computer program: the use without right of a computer program which is protected by law and which has been reproduced without right, with intent, either to procure an unlawful economic gain for himself or for another person or to cause harm to the holder of the right.

Many elements of these minimum and optional lists have by now found their way into national computer crime legislation, along with significant improvements in criminal investigative powers and procedures necessitated by the challenges of prosecuting cybercrime. In Australia, similar minimum requirements were formulated in early stages of the development of the *Cybercrime Act 2001* (Cth) and its state/territory counterparts (Thompson & Berwick 1997). This legislation also partly reflects the draft COE *Convention on Cybercrime*, which now provides a model for many legislatures both in Europe and elsewhere.

COE Convention on Cybercrime

The Council of Europe's Convention on Cybercrime was opened for signature in November 2001. Signatories include over 40 European countries, as well as (non-member states of the Council of Europe) Canada, Japan, South Africa and the United States. The convention required five ratifications to come into force, which occurred on 1 July 2004. To date, 15 member countries (all European) have ratified or acceded to the convention, while 28 countries have signed but not ratified. After a long period of consideration, the United States Senate agreed to ratify the convention on 4 August 2006.

The comprehensive substantive and procedural provisions of the convention are designed to assist with the harmonisation process, while affording adequate protection for due process and human rights. Categories of cybercrime offences and liability dealt with in Chapter II of the Convention include:

- offences against the confidentiality, integrity and availability of computer data and systems:
  - illegal access
  - illegal interception
  - data interference
  - system interference
  - misuse of devices
- computer-related offences:
  - computer-related forgery
  - computer-related fraud
- content-related offences:
  - offences related to child pornography
- offences related to copyright infringement and related rights
- ancillary liability and sanctions:
  - attempt and aiding or abetting
  - corporate liability
  - sanctions and measures.

Chapter II goes on to canvass procedural matters such as collection and preservation of evidence, production orders, search and seizure, data interception and jurisdictional issues. In particular, the procedural provisions cover:

- expedited preservation of stored data
- expedited preservation and partial disclosure of traffic data
- production orders

- search and seizure of stored computer data
- real-time collection of data traffic
- interception of content data
- jurisdiction.

Chapter III deals with mechanisms for international cooperation, such as extradition and mutual assistance. These provisions supplement existing multilateral and bilateral treaties and arrangements. In particular, the following issues are covered:

- extradition
- mutual assistance
- spontaneous information
- procedures for mutual assistance in the absence of international agreements
- confidentiality and limitation on use
- expedited preservation of stored data
- expedited disclosure of preserved traffic data
- mutual assistance regarding accessing of stored data
- transborder access to stored data with consent or where publicly available
- mutual assistance regarding real-time collection of traffic data
- mutual assistance regarding interception of content data
- 24/7 network.

There is also an optional protocol to the convention, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. This was opened for signature on 28 January 2003, and has attracted a total of 31 signatories, with seven ratifying or acceding. The protocol came into force on 1 March 2006 with its fifth ratification.

Particular provisions of the optional protocol deal with:

- dissemination of racist and xenophobic material through computer systems
- racist and xenophobic motivated threats
- racist and xenophobic motivated insults
- denial, gross minimisation, approval or justification of genocide or crimes against humanity
- aiding and abetting.

The protocol's definition of racist and xenophobic material is:

> … any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

While Australia is not a signatory to the Council of Europe's *Convention on Cybercrime* or the protocol, the convention's earlier drafts were influential in shaping the *Cybercrime Act 2001* (Cth) and subsequent legislation such as the recently enacted telecommunications offences (discussed below), which extend to use of the internet for dissemination of offensive content.

3
Australian legislative framework

Commonwealth, state and territory legislation

In Australia, criminal law is largely the preserve of the state and territory jurisdictions. Accordingly, there are substantive criminal offences relating to many forms of computer misuse in the legislation of each of the state and territory jurisdictions. In addition, there is a growing body of Commonwealth law relating to computer technology, particularly telecommunications systems. These operate alongside general criminal laws, and specific offences under other legislation dealing with such matters as intellectual property rights, classification of publications, terrorism and national security.

The following table provides a summary of Australian computer-related offences (Table 1).

Table 1: Main Australian computer-related offence legislation

	Main computer-related offence provisions	Introduction/ amendment	Maximum penalties
ACT	*Criminal Code 2002*, ss415 – 421 and ss423	Replacing previous computer offences under the *Crimes Act 1900*	ss415: punishable by imprisonment for five years or longer ss416 and s417: punishable by a maximum of 1,000 penalty units, 10 years imprisonment, or both ss418 and ss419: punishable by a maximum of 300 penalty units, three years imprisonment, or both ss420 and ss421: punishable by a maximum of 200 penalty units, two years imprisonment, or both ss423: punishable by a maximum of 2,500 penalty units, 25 years imprisonment, or both
NSW	*Crimes Act 1900*, ss308C – 308I	Added by *Crimes Amendment (Computer Offences) Act 2001*	ss308C: punishable by the maximum penalty applicable if the person had committed, or facilitated the commission of, the serious indictable offence in this jurisdiction ss308D and ss308E: punishable by a maximum of 10 years imprisonment ss308F and ss308G: punishable by a maximum of three years imprisonment ss308H and ss308I: punishable by a maximum of two years imprisonment
NT	*Criminal Code Act*, ss276B – 276E	Added by *Criminal Code Amendment Act 2001*	ss276B – s276D: punishable by the maximum penalty of 10 years imprisonment s276E: punishable by the maximum penalty of three years imprisonment
Qld	*Criminal Code Act 1899*, s408E	Added by *Criminal Law Amendment Act 1997*	ss408E(1): punishable by a maximum of two years imprisonment ss408E (2): punishable by a maximum of five years imprisonment ss408E (3): punishable by a maximum of 10 years imprisonment
SA	*Summary Offences Act 1953*, s44 and s44A Part 4A of the *Criminal Law Consolidation Act 1935*, s86E – 86H	Added by *Summary Offences Act Amendment Act 1989* and amended by *Summary Offences (Offensive and Other Weapons) Amendment Act 1998* *Statutes Amendment (Computer Offences) Act 2004*	s44: punishable by a maximum of another A$2,500 ($2,500 or imprisonment for six months imprisonment if ss44(2)(a) applies) s44A: punishable by a maximum of two years imprisonment s86E and s86F: punishable by the maximum penalty for an attempt to commit the principal offence s86G and s86H: punishable by a maximum of 10 years imprisonment

Table 1: continued

	Main computer-related offence provisions	Introduction/ amendment	Maximum penalties
Tas	*Criminal Code Act 1924*, s257B – 257E *Police Offences Act 1935*, s43A – 43D	Added by *Criminal Law Amendment Act 1990*	s257B – 257E: Criminal Code Act 1924, s454 also states that: 'Except as is otherwise expressly provided, references in any enactment to a sentence of imprisonment passed on any person for a term not less than or exceeding a specified term are to be construed as including references to a sentence of imprisonment passed on that person for the term of his or her natural life.' s43A – 43D: punishable by a maximum of a fine of 20 penalty units and two years imprisonment
Vic	*Crimes Act 1958*, ss247B – 247H, and ss247K – L	Added by *Crimes (Property Damage and Computer Offences) Act 2003*	ss247B: punishable by the maximum penalty as applies to the commission of the serious offence in Victoria. ss247C and ss247D: punishable by a maximum of 10 years imprisonment ss247E and ss247F: punishable by a maximum of three years imprisonment ss247G and ss247H: punishable by a maximum of two years imprisonment ss247K: punishable by a maximum of 25 years imprisonment ss247L: punishable by a maximum of 15 years imprisonment
WA	*Criminal Code*, ss440A(3)(a) – 440A(3)(c)	Added by *Criminal Law Amendment (Simple Offences) Act 2004*	ss440A(3)(a): punishable by a maximum of 10 years imprisonment ss440A(3)(b): punishable by a maximum of five years imprisonment ss440A(3)(c): punishable by a maximum of two years imprisonment (12 months imprisonment and a fine of $12,000 if summary conviction applies)

Sources: Compiled from legislative databases including http://www.comlaw.gov.au/, http://www.legislation.act.gov.au/, http://www.legislation.nsw.gov.au/, http://www.nt.gov.au/dcm/legislation/current.html, http://www.legislation.qld.gov.au/OQPChome.htm, http://www.legislation.sa.gov.au/index.aspx, http://www.thelaw.tas.gov.au/index.w3p, http://www.dms.dpc.vic.gov.au/ and http://www.slp.wa.gov.au/statutes/swans.nsf

Although s222 (Unlawfully obtaining confidential information) of the Northern Territory *Criminal Code*, added in 1983 and still in force is not specific to computer-related offences, this offence would apply if the person in question 'unlawfully abstracts any confidential information from any register, document, computer or other repository of information ... with intent to publish the same to a person who is not lawfully entitled to have or to receive it'. The first prosecution under this provision involved an employee of the NT Police who had provided names and addresses from a police database to her de facto husband, a private investigator: *Snell v Pryce* [1990] NTSC 2 (15 February 1990).

Early state and territory computer offences were aimed largely at unauthorised intrusion into computer databases (called computer trespass in a (now repealed) Victorian provision, s9A of the *Summary Offences Act 1966* (Vic)), considered in cases such as *DPP v Murdoch* (1993) 1 VR 406. These offences were similar to traditional property offences such as theft and criminal damage, with the difference that the property being protected was computers and computer data. The key element in such offences was unauthorised access to, or use or modification of, data.

The Commonwealth enacted its own computer offences in 1986, in Part VIA (comprising ss76A – 76F) of the *Crimes Act 1914* (Cth). These offences criminalised unlawful access to or impairment of Commonwealth computers and data, and carried penalties up to 10 years imprisonment. Persons prosecuted under the latter provisions included public servants and contractors who dishonestly used their access to Commonwealth computers and data to facilitate unauthorised benefits for themselves or other persons (Smith, Grabosky & Urbas 2004).

As a result of reforms to Commonwealth criminal law commenced in the 1990s under the auspices of the Model Criminal Code Officers Committee (MCCOC) of the Standing Committee of Attorneys-General (SCAG), the *Crimes Act 1914* computer offences were updated and relocated to the *Criminal Code Act 1995* (Cth) with the coming into force of the *Cybercrime Act 2001* (Cth). In introducing the Cybercrime Bill, the then Attorney-General explained (Second Reading, House of Representatives, 27 June 2001):

> More than 3 million Australian households and over 1 billion people worldwide are connected to the Internet. With the exponential growth in the Internet population and in electronic commerce over the last decade, the integrity, security and reliability of computer data and electronic communication is becoming increasingly important.
>
> Cybercrime activities, including hacking, virus propagation, denial of service attacks and website vandalism, pose a significant threat to the integrity and security of computer data. Indeed, according to recent estimates, cybercrime is costing companies worldwide approximately 3 trillion dollars a year.
>
> Updated laws are vital if authorities are to effectively detect, investigate and prosecute cybercrime activities. The proposed new computer offences and investigation powers in this Bill are a significant development in the fight against these activities and will place Australia at the forefront of international efforts to address the issue of cybercrime.
>
> With the enactment of the *Cybercrime Act* and more recent telecommunications offences (discussed below), the Commonwealth has notably expanded its jurisdictional reach into areas of criminal law that have hitherto been the responsibility of the states and territories. It can be expected, therefore, that more Australian prosecutions for technology-enabled crimes will be pursued under Commonwealth rather than state and territory laws.

Model Criminal Code project and the *Cybercrime Act 2001*

In 1990, a project was established by the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General which comprised senior law officers from all jurisdictions. The Commonwealth enacted general Model Criminal Code principles of criminal responsibility in Chapter 2 of the *Criminal Code Act 1995* (Cth), and subsequent amendments have progressively added substantive provisions. These now include:

- offences relating to bribery of foreign officials, offences against United Nations and associated personnel, international terrorist activities using explosive or lethal devices, and people smuggling (Chapter 4 – The integrity and security of the international community and foreign governments)
- treason and espionage, terrorist acts and organisations, financing terrorism, and harming Australians overseas (Chapter 5 – The security of the Commonwealth)
- theft, fraud and other property offences, forgery, bribery and offences against Commonwealth public officials (Chapter 7 - The proper administration of Government)
- offences against humanity, war crimes, slavery and sexual servitude, trafficking in persons and debt bondage (Chapter 8 – Offences against humanity and related offences)
- serious drug offences, dangerous weapons and contamination of goods (Chapter 9 – Dangers to the community)
- money laundering, postal, telecommunications, computer and financial information offences (Chapter 10 – National infrastructure).

In January 2001, the Model Criminal Code Officers Committee published its *Report on Damage and Computer Offences* (MCCOC 2001). Based on this report, the Cybercrime Bill 2001 was introduced into the Commonwealth Parliament on 27 June 2001, and with some amendments after consideration by the Senate Legal and Constitutional Committee, was enacted.

The *Cybercrime Act 2001* (Cth) came into effect on 1 October 2001, adding new provisions to the *Criminal Code Act 1995* (Cth), *the Crimes Act 1914* (Cth) and the *Customs Act 1901* (Cth). Thus the *Cybercrime Act* served both to modernise Commonwealth computer offences (previously largely contained in the *Crimes Act 1914*) and to provide a model for the states and territories.

The main provisions that were added to the *Criminal Code Act 1995* by the *Cybercrime Act 2001* are those contained in Part 10.7, in particular in Division 477 – Serious computer offences. In particular:

- ss477.1 creates an offence of using a carriage service and causing unauthorised access, modification or impairment with intention to commit any serious Commonwealth, state or territory offence (the term carriage service has the same meaning as in the *Telecommunications Act 1997* (Cth), a serious offence is one punishable by life or five years imprisonment or more, and the penalty for a s477.1 offence is as for the serious offence)
- ss477.2 creates an offence of unauthorised modification of data to cause impairment, where the data or computer involved are Commonwealth data or computers, or the modification is by means of a carriage service (defined as for s477.1), carrying a penalty of 10 years imprisonment
- ss477.3 creates an offence of unauthorised impairment of electronic communication, also punishable by 10 years imprisonment.

Division 478 – Other computer offences, also added by the Cybercrime Act, contains a number of less serious offences, punishable by two or three years imprisonment.

- ss478.1 creates an offence of unauthorised access to, or modification of, restricted data; punishable by two years imprisonment
- ss478.2 creates an offence of unauthorised impairment of data held on a computer disk, etc; punishable by two years imprisonment
- ss478.3 creates an offence of possession or control of data with intent to commit a computer offence; punishable by three years imprisonment
- ss478.4 creates an offence of producing, supplying or obtaining data with intent to commit a computer offence; punishable by three years imprisonment
- ss480.4 creates an offence of dishonestly obtaining or dealing in personal financial information; punishable by five years imprisonment
- ss480.5 creates an offence of possession or control of thing with intent to dishonestly obtain or deal in personal financial information; punishable by three years imprisonment

With some divergences, the Commonwealth model has been followed in a number of states and territories:

- The Australian Capital Territory followed with the *Criminal Code 2002* (ACT), which incorporates both the Model Code computer offences and the general principles of criminal responsibility.
- New South Wales added computer offences based on the Model Code provisions with its *Crimes Amendment (Computer Offences) Act 2001* (NSW), though it has not (yet) enacted the Model Code's general principles of criminal responsibility and so the statutory offences must be interpreted largely against a common-law background (Steel 2002, Bronitt & Gani 2003).
- In 2002 the Northern Territory also enacted new computer offences in its Criminal Code, based on the Model Code provisions (Bronitt & Gani 2003).

- Victoria followed with its *Crimes (Property Damage and Computer Offences) Act 2003* (Vic), largely replicating the Model Code offences (Bronitt & Gani 2003).
- Finally, South Australia introduced similar legislation the following year: *Statutes Amendment (Computer Offences) Act 2004* (SA), in force from 30 May 2004.

Recent Commonwealth telecommunications offences

Apart from its role in providing a model set of computer crime provisions for the states and territories, the *Cybercrime Act 2001* significantly expanded the Commonwealth's coverage of computer-related crime by using the constitutional power under s51(v) of the Constitution with respect to 'postal, telegraphic, telephonic, and other like services'.

The same constitutional power over the misuse of a carriage service, which effectively includes the internet, features in a range of new offences added to the *Criminal Code Act 1995* (Cth) by the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act 2005* (Cth), which came into force on 6 July 2005. This added a new Part 10.6 to the *Criminal Code Act 1995* (Cth), containing new offences prohibiting the misuse of telecommunications networks for a range of illicit purposes, including:

- with the intention of committing a serious offence (s474.14)
- to make a threat (s474.15)
- to make a hoax threat (s474.16)
- to menace, harass or cause offence (s474.17)
- to misuse an emergency call service (s474.18)
- to access or transmit child pornography material (s474.19)
- to possess, control, produce, supply or obtain child pornography material (s474.20)
- to access or transmit child abuse material (s474.22)
- to possess, control, produce, supply or obtain child abuse material (s474.23)
- to procure a person under 16 years of age for sexual purposes (s474.26)
- to groom a person under 16 years of age for sexual purposes (s474.27).

In addition, a new offence of using a carriage service for suicide related material was added by the *Criminal Code Amendment (Suicide Related Material Offences) Act 2005* (Cth), with effect from 6 January 2006.

The main elements of these offences, together with maximum penalties, are set out below (Table 2).

Table 2: Main telecommunications offences under Division 474 of the *Criminal Code Act 1995* (Cth)

Section and heading	Main elements/defences	Maximum penalty
474.4 Interception devices	Unauthorised manufacture, sale, possession etc. of an interception device	Five years
474.5 Wrongful delivery of communications	Causing a communication to be received by a person or service other than the person or service to whom it is directed	One year
474.6 Interference with facilities	Interfering with facility owned by a carrier, carriage service provider	One year
	If the interference results in hindering normal service	Two years
474.7 Modification of a telecommunications device identifier	Unauthorised modification of or interference with a telecommunications device identifier	Two years
474.10 Copying subscription-specific secure data	Copying such data from an account identifier onto a new identifier, etc.	Two years
474.14 Using a telecommunications network with intent to commit a serious offence	Connecting to or using a telecommunications network with intention to commit or facilitate the commission of a serious offence under Commonwealth, state or territory or foreign law (carrying penalty of five years or more)	As for the serious offence
474.15 Using a carriage service to make a threat	Threat to kill	10 years
	Threat to cause serious harm	Seven years
474.16 Using a carriage service for a hoax threat	Intention of inducing false belief that explosive etc. has been left in any place	10 years
474.17 Using a carriage service to menace, harass or cause offence	Whether by method of use or content of communication, using a carriage service in a way that reasonable persons would regard as menacing, harassing or offensive	Three years
474.18 Improper use of emergency call service	Making false or vexatious calls to emergency services number	Three years
474.19 Using a carriage service for child pornography material	Intentional use of a carriage service, with recklessness as to the transmission etc. of child pornography material	10 years
472.20 Possessing, controlling, producing, supplying or obtaining child pornography material for use through a carriage service	Defences of public benefit such as law enforcement and approved research uses are found in s474.21	
474.22 Using a carriage service for child abuse material	Intentional use of a carriage service, with recklessness as to the transmission etc. of child abuse material	10 years
472.23 Possessing, controlling, producing, supplying or obtaining child abuse material for use through a carriage service	Defences of public benefit such as law enforcement and approved research uses are found in s474.24	
474.25 Obligations of internet service providers and internet content hosts	Must refer to Australian Federal Police details of any material that the ISP or ICH has reasonable grounds to believe is child pornography or child abuse material	100 penalty units ($11,000 for an individual or $55,000 for a corporation)
474.26 Using a carriage service to procure persons under 16 years of age	Transmitting a communication with intention of procuring a person under 16 for sexual activity	15 years
	Defences as to belief in age of person etc. are found in s474.29	
474.27 Using a carriage service to groom persons under 16 years of age	Transmitting a communication containing indecent material with intention of making it easier to procure a person under 16 for sexual activity	12 years
	Defences as to belief in age of person etc. are found in s474.29	

Table 2: continued

Section and heading	Main elements/defences	Maximum penalty
474.29A Using a carriage service for suicide-related material	Using a carriage service to access, transmit, make available, publish or otherwise distribute material that directly or indirectly promotes or provides instruction on a particular method of committing suicide, intending that another person promote or provide instruction on the method or use the material to commit suicide	1000 penalty units ($110,000 for an individual or $550,000 for a corporation)

Note: One penalty unit is equivalent to $110: *Crimes Act 1914* (Cth), s4AA. The terms carriage service, telecommunications network, internet content host , internet service provider and interception device are as respectively defined in the *Broadcasting Services Act 1992* (Cth), *Telecommunications Act 1997* (Cth) and T*elecommunications (Interception) Act 1979* (Cth).

Source: Compiled from legislative databases including AustLII: http://www.austlii.edu.au/ and Comlaw: http://www.comlaw.gov.au/

The drafting of some of these offences is notably broad. For example, s474.14, criminalises the use of a telecommunications network to commit a serious Commonwealth, state or territory (or even foreign) offence. The maximum punishment is as for the serious offence, which is defined to be any offence carrying a penalty of life imprisonment or five or more years. However, unlike s477.1 (discussed above), there is no requirement of unauthorised access, modification or impairment – thus, the use of the telecommunications network (including the internet) may be authorised and quite legal, but it is still an offence if this use is accompanied by an intention through this connection to commit a serious offence.

The explanatory memorandum to the Bill introducing s474.14 described its intended scope as follows:

> Proposed subsection 474.14(1) will cover a broad range of preparatory activities that make use of telecommunications, undertaken with the intention to commit, or facilitate the commission of, a serious offence. Connected, as defined in proposed section 473.1, includes connection otherwise than by means of physical contact, for example connection by radiocommunication. This means the proposed offence extends to, for example, the wireless connection of a mobile phone or other device to a telecommunications network with the requisite intention, as well as the physical connection to a telecommunications network of, for example, network maintenance equipment, a telephone or a computer.

The proposed offence under subsection 474.14(2) will cover any use of equipment connected to a telecommunications network to commit, or facilitate the commission of, an offence. Examples of the type of conduct covered by the proposed offence range from the simple making of a telephone call to facilitate the commission of a bank robbery to the use of a computer connected to the Internet to electronically remove money from a financial institution's computer system.

It can be expected that s474.14 will largely displace the need to use previously enacted unauthorised access offences such as s477.1, discussed above. With these new telecommunications offences, it is also likely that Commonwealth authorities will assume a more dominant role in the investigation and prosecution of cybercrime offences. For example, in March 2006, the AHTCC reported that a Melbourne man had been charged with botnet-related activities after a joint investigation by the AHTCC, the Australian Federal Police (AFP), and New South Wales and Victoria Police. Initial information was provided by the Belgian Federal Computer Crime Unit following a series of DDoS attacks on IRC servers in Australia, which also affected the United States Singapore and Austria. The suspect, a 22-year-old male, faces charges under s474.14 of the *Criminal Code Act 1995* (Cth), which creates an offence of using a telecommunications network (such as the internet) with intention to commit a serious offence (AHTCC 2006).

Other offences in Part 10.6 are also capable of application to a range of conduct not previously covered by Commonwealth criminal law, such as child pornography and grooming, and racial vilification. These are discussed further below.

Financial information offences

The *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004* (Cth) also added Part 10.8 – Financial information offences to the *Criminal Code Act 1995* (Cth). This contains a range of offences directed at dishonest dealings with personal financial information or use of devices (such as credit card skimmers) to obtain such information without consent. The term personal financial information means:

> information relating to a person that may be used (whether alone or in conjunction with other information) to access funds, credit or other financial benefits.

Of these offences, s480.4 is broadly framed to apply where a person dishonestly obtains or deals in personal financial information without consent, punishable by imprisonment for five years. This offence would apply to phishing activities, as well as many other forms of identity theft or fraud. The offences under s480.5 and s480.6 respectively apply to possession or control and importation of devices such as credit card skimmers with the intention to dishonestly obtain or deal in personal financial information, punishable by imprisonment for three years.

Specific identity crime offences

Stolen, created or lent identities, obtained fraudulently or fabricated, have been used to facilitate other crimes such as frauds and terrorism. For example, in the 13 December 2001 terrorist attack on India's parliament house complex in which eight security personnel, one civilian and five terrorists were killed, police recovered evidence showing that the laptop had been used to make forged identity cards found on the bodies of the terrorists who were killed in the attack:

> Six fake identity cards purportedly issued by Xansa Websity, 37, Bungalow Road, New Delhi to different students with their address as 120-A, Adarsh Nagar, Delhi and the telephone number as 9811489429. These identity cards were in the names of Anil Kumar, Raju Lal, Sunil Verma, Sanjay Koul, Rohail Sharma and Rohail Ali Shah (which were subsequently found to be fake names of the deceased terrorists) (*State (N.C.T. of Delhi) v Navjot Sandhu* (4 August 2005))

In another more recent example, Gregory A White of Strongsville, Ohio, allegedly 'opened at least 35 brokerage accounts via the [i]nternet at Ameritrade and E*Trade, using the names, Social Security account numbers, dates of birth and other personal identifying information of other individuals without their knowledge, using fraudulent Electronic Funds Transfers from various banks in the Cleveland area, and elsewhere' (US DoJ 2007b). The indictment included allegations that 50 interstate Electronic Funds Transfers from various banks to Ameritrade and E*Trade totalling approximately US$3,348,000had been made.

Although some of the existing offences under Commonwealth, state and territory laws could be applied to identity-related crimes, only Queensland and South Australia currently have provisions that specifically criminalise such crime.

Section 408D of the *Criminal Code Act 1899* (Qld) makes it an offence to obtain or deal with another entity's identification information for the purpose of committing or facilitating the commission of an indictable offence; punishable by a maximum of three years imprisonment.

The following provisions in Part 5A of the *Criminal Law Consolidation Act 1935* (SA) criminalise the following conduct:

- s144B makes it an offence to assume a false identity (including falsely pretending to have a particular qualification or have, or be entitled to act in, a particular capacity) with the intent to commit, or facilitate the commission of, a serious criminal offence; punishable by a penalty appropriate to an attempt to commit the serious criminal offence
- s144C makes it an offence to misuse personal identification information with the intent to commit, or facilitate the commission of, a serious criminal offence; punishable by a penalty appropriate to an attempt to commit the serious criminal offence
- ss144D(1) makes it an offence to produce or has possession of prohibited material, with the intent to use the material, or to enable another person to use the material, for a criminal purpose; punishable by a maximum of three years imprisonment
- ss144D(2) makes it an offence to sell (or offer for sale) or give (or offer to give) prohibited material to another person, knowing that the other person is likely to use the material for a criminal purpose; punishable by a maximum of three years imprisonment
- ss144D(3) makes it an offence to has possession of equipment for making prohibited material intending to use it to commit an offence; punishable by a maximum of three years imprisonment.

The following provisions in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) could also be applied to identity crime.

- s137 makes it an offence for a person to provide false or misleading documents; punishable by a maximum of 10 years imprisonment or 10,000 penalty units, or both.
- ss138(1) makes it an offence for a person to make a false document with the intention that the person or another will produce the false document in the course of an applicable customer identification procedure and the applicable customer identification procedure is under this Act; punishable by a maximum of 10 years imprisonment or 10,000 penalty units, or both.
- ss138(3) makes it an offence for a person to knowingly possess a false document with the intention that the person or another will produce it in the course of an applicable customer identification procedure; and the applicable customer identification procedure is under this Act; punishable by a maximum of 10 years imprisonment or 10,000 penalty units, or both.
- ss138(5) makes it an offence for a person to possess equipment for making a false document knowing that a device, material or other thing is designed or adapted for the making of a false document (whether or not the device, material or thing is designed or adapted for another purpose); and has the device, material or thing in his or her possession with the intention that the person or another person will use it to commit an offence against ss138(1); punishable by a maximum of 10 years imprisonment or 10,000 penalty units, or both.
- ss138(6) makes it an offence for a person to make or adapt a device, material or other thing; and knows that the device, material or other thing is designed or adapted for the making of a false document (whether or not the device, material or thing is designed or adapted for another purpose); and makes or adapts the device, material or thing with the intention that the person or another person will use it to commit an offence against ss138(1); punishable by a maximum of 10 years imprisonment or 10,000 penalty units, or both.

To ensure that crimes involving the criminal misuse of identity can be prosecuted in each jurisdiction, the Australian Government is considering the introduction of legislation that will criminalise activities associated with identity crime (e.g. identity theft and fraud), onselling of identity data, and possessing equipment to create identification information (MCLOC 2007).

Cyberterrorism offences

In addition to the main computer offence provisions discussed above, there are various other offences that may apply to the misuse of computers or criminality directed against telecommunications systems. For example, the main terrorism offence under Commonwealth law, s101.1 (Terrorist acts) of the *Criminal Code Act 1995* (Cth), provides that a person who commits a terrorist act is liable to imprisonment for life. A terrorist act is defined in s100.1 (Terrorist acts) of the *Criminal Code Act 1995* (Cth) – as inserted by the *Security Legislation Amendment (Terrorism) Act 2002* (Cth) – as an action or threat of action causing serious harm to persons or property, or endangering life or public safety, accompanied by the intention of advancing a political, religious or ideological cause, and done to intimidate an Australian or foreign government or the public. The Commonwealth definition of terrorist act was subsequently adopted by other states and territories, such as the *Terrorism (Extraordinary Temporary Powers) Act 2006* (ACT), *the Terrorism (Police Powers) Act 2002* (NSW) and the *Terrorism (Emergency Powers) Act* (NT).

Of particular interest is the fact that this definition explicitly covers any act or threat that 'seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:

(i) an information system

(ii) a telecommunications system

(iii) a financial system

(iv) a system used for the delivery of essential government services

(v) a system used for, or by, an essential public utility

(vi) a system used for, or by, a transport system.'

Thus, cyberterrorism is covered by the terrorist offence provisions, at least insofar as sabotage of telecommunications and similar attacks are concerned. Such acts would fall within the definition of a terrorist act if accompanied by the requisite political or similar intentions, and would be punishable by life imprisonment under s101.1 (Terrorist acts) of the *Criminal Code Act 1995* (Cth). In addition, there are provisions directed at the suppression of terrorist financing that may well apply predominantly to the online fund-raising activities of some groups (Urbas 2005).

Other terrorist offence provisions included in the *Criminal Code Act 1995* (Cth) (as amended by the *Criminal Code Amendment (Terrorist Organisations) Act 2002* (Cth), the *Criminal Code Amendment (Terrorism) Act 2003* (Cth), and the *Anti-Terrorism Act 2005* (Cth)) include:

- s101.2 makes it an offence to provide or receive training connected with terrorist acts; punishable by a minimum of 15 years imprisonment and a maximum of 25 years imprisonment
- s101.4 makes it an offence to possess things connected with terrorist acts; punishable by a minimum of 10 years imprisonment and a maximum of 15 years imprisonment
- s101.5 makes it an offence to collect or make documents likely to facilitate terrorist acts; punishable by a minimum of 10 years imprisonment and a maximum of 15 years imprisonment
- s101.6 makes it an offence to do any act in preparation, or planning, terrorist acts; punishable by life imprisonment

Each of the sections listed in one for which the jurisdiction is extended, by operation of s15.4 (extended geographical jurisdiction—category D) of the *Criminal Code Act 1995* (Cth) to actions wherever they occur (not limited to Australia).

Although most terrorism offences are governed by Commonwealth legislation rather than by state and territory legislation, terrorism-related acts may constitute offences under existing state and territory law. For example, s310J of the *Crimes Act 1900* (NSW) makes it an offence to be a member of a terrorist organisation knowingly. *The Terrorism (Police Powers) Act 2002* (NSW), amended by the *Terrorism Legislation Amendment (Warrants) Act 2005* No. 54, provides powers for NSW police officers to prevent and investigate terrorist-related acts.

Clear examples of cyberterrorism activities are rare, either in Australia and internationally, though any instance of technology-enabled crime that exposes vulnerabilities in critical infrastructure security indicates the potential for a cyberterrorist attack. An example is the case of Vitek Boden, who used wireless access to hack into a Queensland sewage system, causing millions of litres of untreated sewage to spill into rivers and parks: *R v Boden* [2002] QCA 164 (10 May 2002).

More likely, however, are aspects of planning or preparation for terrorist activities that involve some use of computer technology. In July 2006, Faheem Khalid Lodhi was convicted of offences including plotting in October 2003 to bomb the national electricity grid in the cause of violent jihad. Part of the prosecution case was that he had downloaded information including electricity grid maps from the internet. Lodhi was sentenced to 20 years in prison on 23 August 2006: *Regina v Lodhi* [2006] NSWSC 691 (23 August 2006). Terrorists, for example, could simply use open-source geospatial information to plan attacks on military forces stationed overseas (Choo, Smith & McCusker 2007). Terrorists might have used information obtained from Google Earth™ to facilitate their planning of physical attacks against British troops in Iraq as recently reported:

> [d]ocuments seized during raids on the homes of insurgents last week uncovered print-outs from photographs taken from Google. The satellite photographs show in detail the buildings inside the bases and vulnerable areas such as tented accommodation, lavatory blocks and where lightly armo[u] red Land Rovers are parked (Harding 2007).

In another technology-enabled example, it was reported that:

> from approximately 1997 through at least August 2004, British nationals Babar Ahmad, Syed Talha Ahsan, and others, through an organization based in London called Azzam Publications, are alleged to have conspired to provide material support and resources to persons engaged in acts of terrorism through the creation and use of various Internet Websites, email communications, and other means. One of the means Ahmad and his co-conspirators are alleged to have used in this effort was the management of various Azzam Publications websites, principally www.azzam.com <file:///\\www.azzam.com>, which, along with associated administrative email accounts, were hosted for a period of time on the servers of a Web hosting company located in the state of Connecticut (US DoJ 2007d)

Intellectual property offences

Criminal offences for intellectual property infringement are found in the *Copyright Act 1968* (Cth) and *Trade Marks Act 1995* (Cth). Unlike some other countries, Australia does not have offences of patent infringement, design infringement, breach of confidence or circuit layouts infringement (Urbas 2000). There is also an infringement offence in s74 of the *Plant Breeder's Rights Act 1994* (Cth), punishable by a fine only (which appears to have never been used).

Offences under the *Copyright Act 1968* (Cth) include commercial dealings (such as making for sale or hire) an infringing article where it is known, or ought reasonably to be known, that the article is infringing (s132). Maximum penalties for most criminal copyright infringement offences are 550 penalty units and/or imprisonment for not more than five years, or five times this amount if the infringer is a corporation (1 penalty unit currently equals $110). The maximum monetary penalty increases to 850 penalty units where the article is infringing because it was made by converting a work or other subject matter from analog or hard copy into digital or machine-readable form (s132(6AA)). Thus, there is a premium for digital copyright infringement.

Under amendments made by the *Copyright Amendment (Digital Agenda) Act 2000* (Cth), there are also offences relating to commercial dealings in broadcast decoding devices, with maximum penalties again reaching 550 penalty units and/or imprisonment for not more than five years (s135AS). The fault element for this category of offences includes recklessness as to whether a device will be used to gain unauthorised access to encoded broadcasts.

Factors determining whether a person has infringed Section 101 of the *Copyright Act 1968* (Cth) are provided for in by ss36(1A) and ss101(1A) as follows:

- the extent (if any) of the person's power to prevent the doing of the act concerned
- the nature of any relationship existing between the person and the person who did the act concerned
- whether the person took any other reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice.

For there to be an infringement of the Act, the alleged infringing act(s) must be sufficiently connected to Australia as provided by ss36(1):

Subject to this Act, the copyright in a literary, dramatic, musical or artistic work is infringed by a person who, not being the owner of the copyright, and without the licence of the owner of the copyright, does in Australia, or authorises the doing in Australia of, any act comprised in the copyright.

Penalties under the *Trade Marks Act 1995* (Cth) are somewhat lower (s149): 500 penalty units and/or imprisonment for not more than two years (again, a corporation may be fined five times this amount). Offences attracting this penalty include falsification of a registered trade mark in the course of trade (s145), and selling goods which are falsely marked (s148). The fault element is knowledge or recklessness as to the falsification.

There have been few prosecutions for criminal copyright or trademark infringement in Australia involving the use of computers or the internet, despite the apparently widespread activity of downloading copyright material such as films, music or software programs without permission of the right holder.

- One case in 2003 concerned three students at the University of Technology, Sydney, who developed a free music download website using the Motion Picture Expert Group 1, Audio Layer 3 (MP3) technology – MP3 WMA land – and made copyright material available on the site. The site was said to have received some seven million hits. The charges were heard in the Central Local Court in Sydney in December 2003, and all three were convicted, with two sentenced to prison terms of 18 months, suspended for three years, and 200 hours community service. The third was assessed as unsuitable for a community service order and was fined $5000 (HTCB no. 3).
- In the case of *Universal Music Australia Pty Ltd v Cooper* [2005] FCA 972 (14 July 2005), the Federal Court found that there had been an infringement of copyright by Stephen Cooper (MP3s4free.net), Camperdown-based ISP E-Talk Communications (trading as ComCen Internet Services), Liam Francis Bal (director of E-Talk/Com-Cen), and Chris Takoushis (employee of E-Talk/Com-Cen) for creating hyperlinks to third-party websites that had infringing sound recordings. In this particular case, the respondents neither stored nor distributed any infringing sound recordings.

It is also an offence to facilitate or circumvent access control technological protection measure under provisions in Divison 2A (Actions in relation to technological protection measures and electronic rights management information) of the *Copyright Act 1968* (Cth).

- s116AN makes it an offence for a person to circumvent an access control technological protection measure if (a) the work or other subject matter is protected by an access control technological protection measure; and (b) the person does an act that results in the circumvention of the access control technological protection measure; and (c) the person knows, or ought reasonably to know, that the act would have that result

- s116AO makes it an offence for a person to (i) manufacture a circumvention device for a technological protection measure with the intention of providing it to another person; (ii) import such a device into Australia with the intention of providing it to another person; (iii) distribute the device to another person; (iv) offer the device to the public; (v) provide the device to another person; (vi) communicate the device to another person; and the person knows, or ought reasonably to know, that the device is a circumvention device for a technological protection measure; and the work or other subject matter is protected by the technological protection measure.
- s116AP makes it an offence for a person to provide a service to another person; or offers a service to the public; and the person knows, or ought reasonably to know, that the service is a circumvention service for a technological protection measure; and the work or other subject matter is protected by the technological protection measure.

For prosecutions involving circumvention devices, it is important to establish whether the copyright work was protected by a technological protection measure as illustrated in the case of *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2002] FCA 906 (26 July 2002). Mr Justice Sackville noted that

> [o]n the evidence, I would have held that the chips installed by Mr Stevens had only a limited commercially significant use other than circumventing or facilitating the circumvention of the access code. Thus, if the access code had been a 'technological protection measure', the chips would have been circumvention devices. I would also have found that Mr Stevens sold or promoted (through advertisements in the Trading Post) the circumvention devices and that he knew that the devices would be used to circumvent or facilitate the circumvention of a technological protection measure.

A notable set of legal proceedings involving an Australian resident, though commenced by United States rather than Australian authorities, is the attempted extradition of an alleged internet software piracy ringleader in New South Wales. He is alleged to have taken a leading role in the global activities of the group DrinkOrDie which has been credited with well-publicised activities involving cracking (i.e. stripping of technological anti-copying protections) and distribution of commercial computer software (Hayes 2006). Federal Court appeals against extradition have been unsuccessful, and the High Court has refused special leave to appeal: see *United States of America v Griffiths* [2004] FCA 879 (7 July 2004); *Griffiths v United States of America* [2005] FCAFC 34 (10 March 2005); and *Griffiths v United States of America & Anor* [2005] HCA Trans 666 (2 September 2005). He was extradited from Australia to the United States in February 2007 (US DoJ 2007f) and pleaded guilty in April 2007 before U.S. District Judge Claude M. Hilton to one count of conspiracy to commit criminal copyright infringement and one count of criminal copyright infringement (US DoJ 2007c). On 22 June 2007, Griffiths was sentenced to 51 months imprisonment (US DoJ 2007d).

Spam provisions

Spam is the electronic equivalent of junk mail which is unsolicited, usually sent in bulk transmissions of thousands or even millions of messages at a time, and significantly impedes the flow of legitimate internet traffic around the world. As at April 2005, the spam statistical report released by Symantec (2005) indicated that 61 percent of global email is identified as spam. Spam is facilitated by the automated harvesting of email addresses from websites, email accounts and – to an increasingly significant extent – by spyware and botnets. The unavailability of a major botnet was suspected to have attributed to a significant 30 percent drop in the number of spam emails detected in the first week of January 2007 (Broersma 2007). Some spam advertises harmless though usually unwanted products such as personal finance or consumer goods, but some offers adult products and pornography (McCusker 2005).

Because this type of content is unsolicited and is often offensive, internet regulators and legislators have begun to place controls on spam activity, such as the *Broadcasting Services Act 1992* (Cth) and the *Spam Act 2003* (Cth).

Schedule 5 of the *Broadcasting Services Act 1992* (Cth) allows Australian residents, body corporations that carry on activities in Australia; or the Commonwealth, a state or a territory to register their complaints on the website of the Australian Communications and Media Authority (https://web.acma.gov.au/secure/complaint_form.htm) about prohibited or potentially prohibited contents (including spam) hosted on the internet. For prohibited content hosted in Australia, the relevant internet content host (ICH) will be liable for a maximum penalty per day of A$5,500 for an individual and A$27,500 per day for a corporation if the ICH fails to comply with a take-down notice by the Australian Communications and Media Authority (ACMA 2007).

The *Spam Act 2003* (Cth), in force from 10 April 2004 and subsequently amended by the *Australian Communications and Media Authority (Consequential and Transitional Provisions) Act 2005* (Cth), which makes it an offence, punishable by civil penalties such as large fines, to send bulk unsolicited email in Australia or to Australian recipients. In one of the first cases to be brought under the *Spam Act* 2003 (Cth), the Australian Communications and Media Authority (ACMA) obtained declaratory orders against a Perth-based business, Clarity1 Pty Ltd, that sent over 200 million unsolicited commercial electronic messages to email addresses that had allegedly been harvested using automated software: *Australian Communications and Media Authority v Clarity1 Pty Ltd* [2006] FCA 410 (13 April 2006). A fine of A$5.5 million was imposed (*Australian Communications and Media Authority v Clarity1 Pty Ltd* [2006] FCA 1399 (27 October 2006), Lebihan 2006). *The Spam Act 2003* (Cth) does not, however, apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication (*Spam Act 2003* (Cth), s44).

The *Spam Act 2003* (Cth) also applies to unsolicited commercial messages sent using short message services (SMS) and multimedia messaging services (MMS). In 2005, two Australian companies – Global Racing Group Pty Ltd and Australian SMS Pty Ltd – were fined A$11,000 and A$2,200 respectively for sending unsolicited commercial SMS messages, breaching the Act (ACMA 2005).

The following provisions under the *Criminal Code 1995* (Cth) may also criminalise spam-related activities (DCITA 2006: 15).

- s477.1 makes it an offence for a person to illegally access a computer and use the computer to send spam without authorisation, which resulted in the impairment of electronic communication to or from a computer (due to the spam activities).
- s477.2 makes it an offence for a person to illegally access a computer and use the computer to send spam without authorisation through third party servers – a typical case in many spoofing attacks.

Some other countries have enacted criminal offences to counteract spamming (e.g. the Spam Control Act 2007 read in the parliament of Singapore on February 2007 and passed in parliament on 12 April 2007). In the United States, several prosecutions have resulted in convictions under the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, which went into effect on 1 January 2004. Within a month of the CAN-SPAM Act's commencement in 2004, the Federal Trade Commission had identified two large-scale spammers from consumer complaints detailing massive numbers of unsolicited messages offering such products as diet patches. Subsequent litigation resulted in settlements including prohibitions on further spamming activity. In one case, the defendant company was based in Australia, and was ordered to disgorge over US$2 million in illicit profits from spamming activities offering human growth hormone products (FTC Media release 20 September 2005).

Cyberstalking and harassment offences

A phenomenon that emerged fairly early with the adoption of the internet and email for personal communication was the misuse of these media for stalking or harassing others. Activities such as obsessively collecting information about a person, sending a person unwanted communications, posting offensive information about a person on the internet, or even hacking into a person's computer to harass them, can all constitute criminal acts under stalking legislation in Australian states and territories (Ogilvie 2000).

Because the internet spans the globe, it is possible to stalk a person far removed from one's physical location. This has led to some jurisdictional complications in applying the law. For example, in *DPP v Sutcliffe* [2001] VSC 43, the Victorian Supreme Court held that a Melbourne man accused of stalking an actress in Canada by means including email was subject to prosecution under s21A of the *Crimes Act 1958* (Vic), which has since been amended to make clear that it extends to cyberstalking which crosses jurisdictional boundaries (Maury 2004).

Misuse of the internet to stalk or harass others may also be dealt with under provisions relating to offensive communications. For example, s474.17 of the *Criminal Code Act 1995* (Cth) creates an offence of using a carriage service to menace, harass or cause offence, which means using the carriage service in such a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive. This provision can be applied to such uses of the internet as the posting of pornographic, defamatory or racist material on websites.

This potential application of the telecommunications offences marks a departure from the coverage of Commonwealth law for many years, which offered only an administrative (non-criminal) complaint mechanism under the *Racial Discrimination Act 1975* (Cth) in regard to racist publications including on the internet: see, for example, *Jones v Toben* [2002] FCA 1150; appeal at *Toben v Jones* [2003] FCAFC 137. The potential application of s474.14, which carries a maximum penalty of three years imprisonment, was recognised in the explanatory memorandum to the Bill:

> Examples of the type of use of a carriage service the proposed offence may cover include use that would make a person apprehensive as to their safety or well-being or the safety of their property, use that encourages or incites violence, and use that vilifies persons on the basis of their race or religion.

The new offence in s474.29A of using a carriage service for suicide related material, added by the *Criminal Code Amendment (Suicide Related Material Offences) Act 2005* (Cth) with effect from 6 January 2006, may also apply to material or discussion that would be regarded as objectionable or offensive by many members of the community.

Existing legislation in some jurisdictions criminalises the use of ICT to stalk or harass others – cyberstalking – as described in Table 3.

Table 3: Summary of cyberstalking offences in Australian states and territories

	Provision	Maximum penalty
ACT	*Crimes Act 1900*, s35	Five years imprisonment if (i) the offence involved a contravention of an injunction or other order made by a court; or (ii) the offender was in possession of an offensive weapon; two years imprisonment otherwise.
Qld	*Criminal Code Act 1899*, s359B	Seven years imprisonment if, for any of the acts constituting the unlawful stalking, the person (a) uses or intentionally threatens to use, violence against anyone or anyone's property; or (b) possesses a weapon within the meaning of the Weapons Act 1990; or (c) contravenes or intentionally threatens to contravene an injunction or order imposed or made by a court or tribunal under a law of the Commonwealth or a state; five years imprisonment otherwise.
NT	*Criminal Code Act*, ss189	Five years imprisonment if (i) the person's conduct contravened a condition of bail or an injunction or order imposed by a court (either under a law of the Commonwealth, the territory, a state or another territory of the Commonwealth); or (ii) the person was, on any occasion to which the charge relates, in the possession of an offensive weapon; two years imprisonment otherwise.
SA	*Criminal Law Consolidation Act 1935*, s19AA	Five years imprisonment for an aggravated offence or three years imprisonment for a basic offence.
Tas	*Criminal Code Act 1924*, s192	Except in capital cases, all sentences are left to the discretion of the judge of the court of trial, who may in any case impose a sentence of imprisonment up to 21 years (Blackwood & Warner 1993). *Criminal Code Act 1924*, s454 states that: except as is otherwise expressly provided, references in any enactment to a sentence of imprisonment passed on any person for a term not less than or exceeding a specified term are to be construed as including references to a sentence of imprisonment passed on that person for the term of his or her natural life.
Vic	*Criminal Code Act 1958*, s21A	10 years imprisonment.

Source: Compiled from legislative databases including http://www.legislation.act.gov.au/ and http://www.nt.gov.au/dcm/legislation/current.html

Child exploitation and grooming offences

Australian states and territories have had obscenity and, more recently, child exploitation (e.g. child abuse materials and child pornography) laws for many years. Examples include:

> Schedule 5 of the *Broadcasting Services Act 1992* (Cth) allows Australian residents, corporations that carry on activities in Australia; the Commonwealth, a state or a territory to register complaints concerning prohibited or potentially prohibited content (including child pornography) hosted on the internet on the website of the Australian Communications and Media Authority (http://www.acma.gov.au/WEB/STANDARD//pc=PC_90103).
>
> Subsection 233BAB(1)(h) of the Customs Act 1901 (Cth) prohibits the importation of items of child pornography or of child abuse material. On 1 August 2007, a visitor from the United Kingdom was arrested and charged with importing prohibited goods in contravention of Regulation 4A of the Customs (Prohibited Imports) Regulations 1956 (Cth) and Section 233BAB of the Customs Act 1901 (Cth) for possessing images depicting child pornography in his laptop computer (Australian Customs Service 2007a). In another more recent case, Bao Peng Lim, a 22 year-old Australian man, was fined A$9,000 after being convicted in Perth Magistrates Court on 13 August 2007 for smuggling child pornography (Australian Customs Service 2007b).

State and territory child pornography laws vary considerably, as do the resources available for their enforcement by police and other agencies (HTCB no. 2 and no. 8; Forde & Patterson 1998). This can be an impediment to national and international investigations, which have emerged as particularly important in disrupting global paedophile networks that operate with a degree of anonymity through internet chat rooms (Grant, David & Grabosky 1997; Krone 2005b).

Commonwealth telecommunications offences include both child pornography and child abuse material offences in ss474.19 – 474.25, and child procuring and grooming offences in ss474.26 – 474.29. Notably, the definition of a child for the purposes of these provisions varies, with the Commonwealth provisions defining child abuse material and child pornography material as involving the depiction of a person who ‘is, or appears to be, under 18 years of age’, while the procuring and grooming provisions relate to a recipient of communications ‘who is, or who the sender believes to be, under 16 years of age’.

In some jurisdictions, it is a separate offence to use ICT to procure or to groom children for the purposes of sexual contact (i.e. procuring offences cover the use of the internet to facilitate a meeting during which the child recipient is intended to engage in sexual conduct with the sender, another adult or another child in the presence of the sender or another adult, and grooming offences cover the sending of an indecent communication to a child with the intention of making it easier to procure the recipient to engage in sexual activity, or making it more likely that the child will engage in or submit to sexual activity with the sender or another person), as described in Table 4. It is notable that no real child need be involved in the commission of this offence, which allows investigators to go online posing as a child (HTCB no. 8). Successful prosecutions of cases involving covert sting operations have also been recorded in other countries such as the United States (e.g. see US DoJ 2007g).

Table 4: Offences relating to the use of ICT to procure or to groom children for the purposes of sexual contact

Jurisdiction	Provision	Maximum penalty	Definition of a child or young person by age
Cth	*Criminal Code Act 1995*, s474.26: Using a carriage service to procure persons under 16 years of age	15 years imprisonment	Under 16 years of age
	Criminal Code Act 1995, s474.27: Using a carriage service to “groom” persons under 16 years of age	12 years imprisonment (15 years imprisonment if ss474.27(3) applies)	Under 16 years of age
NSW	*Crimes Act 1900* (as amended by Crimes Amendment (Sexual Procurement or Grooming of Children) Bill 2007 on 28 November 2007), s66EB: Procuring or grooming child under 16 for unlawful sexual activity	ss66EB(2)(a): 15 years imprisonment	Under 14 years of age
		ss66EB(2)(b): 12 years imprisonment	Under 16 years of age
		ss66EB(3)(a): 12 years imprisonment	Under 14 years of age
		ss66EB(3)(b): 10 years imprisonment	Under 16 years of age
ACT	*Crimes Act 1900*, s66: Using the Internet etc to deprave young people	ss66(1): Ten years imprisonment (five years imprisonment if this is the first offence)	Under 16 years of age
		ss66(3): 100 penalty units, five years imprisonment or both	Under 16 years of age
Qld	*Criminal Code Act 1899*, s218A: Using internet etc. to procure children under 16	ss218A(1): Five years imprisonment	Under 16 years of age
		ss218A(2): 10 years imprisonment	Under 12 years of age
NT	*Criminal Code Act*, s131: Attempts to procure child under 16 years	ss131(1): Three years imprisonment	Under 16 years of age
		ss131(2): Five years imprisonment	Under 16 years of age
	Criminal Code Act, s132: Indecent dealing with child under 16 years	ss132(2): 10 years imprisonment	Under 16 years of age
		ss132(4): 14 years imprisonment	Under 10 years of age
SA	*Criminal Law Consolidation Act 1935*, s63B: Procuring child to commit indecent act etc.	ss63B(1)(a) and ss63B(3)(a): 10 years imprisonment	Under 16 years of age
		ss63B(1)(b) and ss63B(3)(b): 12 years imprisonment	Under 12 years of age
Tas	*Criminal Code Act 1924*, s125D: Communications with intent to procure person under 17 years, etc.	No statutory maximum penalty -- at the discretion of the court with a maximum of 21 years imprisonment (House of Assembly Hansard 2005)	Under 17 years of age
WA	Criminal Code: s204B: Using electronic communication to procure, or expose to indecent matter, children under 16	ss204B(2): Five years imprisonment	Under 16 years of age
		ss204B(3): 10 years imprisonment	Under 13 years of age

Source: Compiled from legislative databases including (Cth) http://www.comlaw.gov.au/, (ACT) http://www.legislation.act.gov.au/, (Qld) http://www.legislation.qld.gov.au/OQPChome.htm, (NT) http://www.nt.gov.au/dcm/legislation/current.html, (SA) http://www.legislation.sa.gov.au/index.aspx, (Tas) http://www.thelaw.tas.gov.au/index.w3p, (WA) http://www.slp.wa.gov.au/statutes/swans.nsf, and (NSW) http://www.legislation.nsw.gov.au/

Commonwealth legislation can be and has been used to prosecute persons in jurisdictions with no specific provision to criminalise online child procurement or child grooming. For example, Richard Gerard Meehan was charged with one count of using a carriage service to transmit communications to a person under 16 years of age with the intention of procuring that person to engage in sexual activity, contrary to ss474.26(1) of the *Criminal Code Act 1995* (Cth), in the Victorian County Court. On 21 July 2006, Meehan was sentenced to 24 months imprisonment, to be released after serving three months of that term in the Victorian County Court (Commonwealth Director of Public Prosecutions 2006, SMH 2006).

In the first investigation under s218A of the *Criminal Code Act 1899* (Qld) after it came into effect on 1 May 2003, Queensland investigators posed as a 13 year-old girl (becky_boo 13) in an internet relay chat room and received emails from a man wanting to engage the girl in sexual activity. They arrested a 25 year-old man when he appeared at an agreed meeting point to meet the girl, only to find that he had been chatting to police all along. After a guilty plea, the defendant was sentenced to imprisonment for two and a half years, suspended after having served nine months. This was reduced on appeal to an 18-month term, suspended from the time of the appeal, the defendant having already served 90 days in custody (*R v Kennings* [2004] QCA 162).

In another Queensland case, however, in which police posed as a 14-year old (Kathy_volleyball), a conviction under s218A was overturned on appeal on the basis that the provision requires that the defendant believed that the person being contacted was under the age of 16 years. In this case, the defendant had given evidence that he had held no belief as to the age of Kathy_volleyball, and the Court of Appeal held that the jury had been misdirected on the application of s218A(8), which provides that evidence that a person (real or fictitious) was represented as being below a certain age is, in the absence of evidence to the contrary, proof that the adult believed the person was under that age: *R v Shetty* [2005] QCA 225 (24 June 2005). A retrial returned a verdict of acquittal in September 2006.

As noted in Table 3, the Commonwealth has recently enacted similar offences relating to child procuring and grooming as part of the recent telecommunications offences added to the *Criminal Code Act 1995* (Cth): s474.26 and s474.27. As with the Queensland offence, there is no requirement that a person under the age of 16 years actually be the target of procuring activity. Further provisions relating to these offences are contained in s474.28 and defences are contained in s474.29 of the *Criminal Code Act 1995* (Cth).

The explanatory memorandum to the Bill introducing these child grooming provisions stated:

> Proposed sections 474.26 - 474.29 contain an offence regime targeting adult offenders who exploit the anonymity of telecommunications services (for example, the Internet) to win the trust of a child as a first step towards the future sexual abuse of that child. The practice is known as 'online grooming'.
>
> There are two steps routinely taken by adult offenders leading up to a real life meeting between adult and child victim that results in child sexual abuse:
>
> (i) The adult wins the trust of a child over a period of time. Adults often use 'chat rooms' on the Internet to do this. They may pose as another child, or as a sympathetic 'parent' figure. Paedophiles reportedly expose children to pornographic images as part of this 'grooming' process. It is proposed to specifically criminalize this practice. Specific offences would remove any doubt about whether online 'grooming' of a child before actual contact is 'mere preparation' (i.e. not a criminal offence) or an unlawful attempt to commit child sexual abuse.
>
> (ii) With the child's trust won, adults often use telecommunications services to set up a meeting with the child. Although this step is more likely to be characterised as an attempt to commit child sexual abuse than step (i), it is desirable to provide a firm justification for police action by enacting specific 'procurement' or 'solicitation' offences. This is consistent with the underlying rationale for the new offences: to allow law enforcement to intervene before a child is actually abused.

Recent instances in which individuals have been charged under Commonwealth, state or territory grooming provisions suggest that they provide a valuable tool for early intervention in child exploitation activity. For example, a man was charged in March 2007 with 'child grooming offences after explicit photographs and messages were allegedly sent to a teenage boy in the United States via the internet' (NSW Police 2007).

Possession of child pornography has been one of the most frequently prosecuted computer-related crimes in recent years (see Smith, Grabosky & Urbas 2004). Recent cases include the arrest of a 21-year-old Manoora in Queensland and a 46-year-old Leonay in Western Sydney man, both with possessing child pornography material, contrary to s228D of the Queensland Criminal Code and s91H (3) of the *Crimes Act 1900* respectively (AFP 2007).

The internet has created a number of issues in relation to what now constitutes possession. Traditionally a person must have possessed a magazine or a physical photograph that involved child pornography to have committed the offence of possession, but with the use of the internet questions have arisen concerning when a person takes possession of images. For example, does the mere act of browsing or viewing such material on a computer constitute the act of possession? As Mr Justice Kennedy observed in Jones (1999) 108 A Crim R 50 at 51:

> In recent times the insidious impact of child pornography has come to be better understood. The problem is an international one, which has been significantly aggravated with the advent of the [i]nternet.

In determining what constitutes possession, the appeal court in *Director of Public Prosecutions v Kear* [2006] NSWSC 1145 (9 October 2006) NSWSC 1145 examined the question of whether by viewing the images the defendant was in possession of a 'film' that would, if classified, be categorised as 'refused classification' under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). The case arose out of Operation Auxin, an international police investigation into the purchase of rights to access child pornography by internet users. This accused in this case had subscribed to the internet website and browsed the site, but had made no identifiable attempt to save the particular material, although it was saved in an independent manner as part of the internet browser application to the internet cache.

The appeal court explained its finding that the defendant did not have possession of the image as follows:

> **(1) Jpeg file in temporary Internet cache a 'film' for purposes of s 578B *Crimes Act* (NSW)**
>
> The question of whether there was evidence to support the charge was a question of law alone though it involved consideration of the meaning of the word film in the section that defines the word for the purposes of s 578B *Crimes Act* (NSW). '[F]or the purpose of s 578B a "film" includes "a cinematograph,......,and any other form of recording from which a visual image, including a computer generated image can be produced". It is also clear that a "computer generated image" is not a film: it is a visual image that is produced from a "film". A computer generated image is "an image...produced by use of a computer monitor......from electronically recorded data". Therefore, it is the "electronically recorded data" in the computer that amounts to a "film" for the purposes of the section.' "'[T]he electronically recorded data" that produced the "computer generated image" viewed by the defendant was the jpeg file' sent by the [Allxboys website to the defendant's computer when he clicked on a page and then on an image to view the image(s) on that web page. Before the thumbnail of the image or its enlarged version could be viewed] the relevant jpeg file had to be sent to the defendant's computer and stored automatically in the temporary Internet cache. It was the jpeg file, transmitted to and stored in the defendant's computer that created the image that he viewed on the monitor…..[W] hat the defendant viewed on the monitor was a "computer generated image". The jpeg file in the temporary Internet cache was a "film" [for the purposes of s 578B *Crimes Act*] because it was a "form of recording from which … a computer generated image can be produced".' While the defendant had film(s) stored on one of his computer hard drives, he did not possess the film(s) because he was unaware of their existence. '[A] "film" must be a recording. … [A] store of information for subsequent reproduction' irrespective of whether its storage is temporary or permanent…. 'If the information is not stored, there is no recording of the information. .. [the information] when viewed by the defendant on the monitor was… merely the retrieval or reproduction of material stored in the jpeg file in the temporary Internet cache.'
>
> **(2) Visual images on monitor did not amount to a recording and defendant's viewing of them insufficient to found charge of possession**
>
> The magistrate's finding that a film under s578B Crimes Act did not include a jpeg file was incorrect. His Honour was however correct in 'finding that the visual image on the monitor was not itself a recording'. On this basis, when the defendant viewed the images he was not 'by that activity alone in possession of a recording.'

4
Jurisdictional, prosecution and sentencing issues

Jurisdictional issues

Traditionally, courts have accepted jurisdiction if a person against whom legal proceedings are brought is physically present in the geographical territory (i.e. country or state) in which the court operates, is a citizen of the territory, or if there is some other sufficient 'territorial nexus'. Such a connection might arise if the alleged victim of a crime is in the territory, or some other effect of the crime sufficient to exercise jurisdiction is present. For crimes involving physical acts, rules of jurisdiction have largely been relatively easy to apply, but the situation is more complicated for online activity.

When a person goes online, he or she may be physically located in *country A*, using computing networks located in *country B*, sending signals that are routed through *country C*, and reaching recipients that are located in *country D*, who may reply to the sender in *country A* and so on. For example, in one incident, Romanian hackers sent an email to the South Pole Research Centre, demanding money with the threat that they would otherwise send details of life-support systems and other data found on the Antarctic facilities' server to another country to expose their vulnerability. The email was traced to a Bucharest internet cafe and two locals were arrested (FBI 2003a).

There have been numerous similar cases involving online fraud, theft of funds, destruction of data, stalking, harassment, ransom and defamation – all committed across jurisdictional borders by means of the internet.

Most computer-related offences under Australian law are governed by legislation that specifies the applicable type of jurisdiction. For Commonwealth computer crimes such as the telecommunications offences and other computer offences in the *Criminal Code Act 1995* (Cth), the specified category is *extended geographical jurisdiction – category A*. This means that a person can be prosecuted in Australia for online conduct if:

- the conduct occurred wholly or partly in Australia
- the conduct occurred wholly or partly on board an Australian ship or aircraft
- the conduct occurred outside Australia but a result of the conduct occurred in Australia or on board an Australian ship or aircraft
- the person is an Australian citizen or a corporation incorporated in Australia
- the offence is ancillary to another offence which is related to or intended to occur in Australia (e.g. attempt or conspiracy).

For some other offences that can be committed using computers, other categories of jurisdiction apply. For example, in Chapter 3.6 of the *Criminal Code Act 1995* (Cth), the definition of terrorist act includes certain types of attack on information, telecommunications, financial and transport systems, but the applicable category is *extended geographical jurisdiction – category D*, which applies:

- whether or not the conduct occurs in Australia
- whether or not a result of the conduct occurs in Australia.

Thus, online offending that constitutes cyberterrorism can be prosecuted under Australian law irrespective of where it occurs, though of course this is unlikely to occur unless Australian citizens or interests are fairly directly affected (Urbas 2005).

Because online offending transcends borders so easily, numerous territories can simultaneously assert jurisdiction. This leads to the necessity of choosing the most appropriate forum for proceedings. This choice can have important consequences due to the different legal systems and penalties that apply in different countries. In a recent online defamation case (*Dow Jones v Gutnick* (2002) 210 CLR 575), the High Court of Australia ruled that a plaintiff in Victoria was able to sue publishers based in the United

States because the publication of allegedly defamatory material occurred where the articles were downloaded from the internet, rather than where it was uploaded to the publisher's server. This meant that the defamation law of Victoria applied, rather than the more constitutionally circumscribed defamation law applying in the defendants' home state (Beyer 2004).

Another consequence of cross-border online offending is that the jurisdiction in which harm has occurred may seek the extradition of an alleged perpetrator from elsewhere. The availability of extradition depends on the agreements that countries make, either bilaterally or as signatories to international conventions relating to particular areas of criminality (e.g. drug trafficking, money laundering, terrorist activity and financing). Australia is signatory to numerous such agreements, and extradition requests have been received in relation to persons said to have been involved in online copyright infringement of software (US DoJ 2003). Conversely, Australia may also request the extradition from other countries of persons who have committed acts online that adversely affect Australian citizens or interests.

Cross-border cooperation

In Australia, as elsewhere, there are two basic forms of international cooperation relating to technology-enabled crime. The first, which might be termed investigator-to-investigator assistance, occurs on an informal basis. Under these circumstances, investigators share information and provide assistance to each other, without reliance on legislation. Such means are appropriate where the information sought is publicly available.

Australia is a member of Interpol, and the AFP has liaison offices in over 30 countries around the world. Interpol facilitates police-to-police assistance and cooperation even where diplomatic relations do not exist between particular countries. The AHTCC hosts a 24/7 network of contacts, enabling nations to alert each other in real time to urgent matters. These arrangements, which allow for a fast freeze, slow thaw process for the preservation of volatile electronic evidence, have been established pursuant to the Council of Europe's *Convention on Cybercrime*. The 24/7 arrangements are available not only to formal signatories to the convention, but also to sympathetic non-signatory states. Although not a signatory to the convention, Australia has formally signed on to these arrangements.

Australia also has a formal regime for mutual assistance in criminal matters, which is governed by the *Mutual Assistance in Criminal Matters Act 1987* (Cth). Formal mutual assistance is invoked when the matter in question entails compulsory powers such as the execution of a search warrant in the requested country, or the extradition of a suspect to the requesting country (Cuthbertson 2001).

While formal mutual assistance can be requested of any country (even in the absence of diplomatic relations), it is usually easier when prior treaty arrangements are in place. Australia has bilateral mutual assistance treaties with 25 countries as of May 2007. However, the machinery of formal mutual assistance is usually fairly slow. Requests must be processed through a central office in both requesting and requested countries, and usually requires approval at a ministerial or other high official level.

Extradition into and out of Australia is governed by the *Extradition Act 1988* (Cth). When an individual situated in Australia commits, or has committed, an offence against a person or institution located in a foreign country, formal extradition machinery may be invoked by the making of an extradition request. to satisfy the criterion of dual criminality, the alleged misconduct must constitute an offence under both foreign and Australian law.

A recently commenced review of Australia's mutual assistance and extradition legislation by the Australian Government Attorney-General's Department noted that reforms may be required to deal with increasingly sophisticated forms of transnational crime, including technology-enabled crime (AGD 2005):

> Crimes committed with or against computers or communications systems are increasing rapidly and traditional crimes such as money laundering and the trafficking of drugs and firearms are being facilitated by new technology.

Although to date, there are no examples of Australians having been extradited overseas, or persons extradited to Australia, in relation to offences that could be characterised as technology-enabled crimes, a British national living in Australia, Hew Raymond Griffiths, has been extradited from Australia to the United States to face criminal charges in connection with operating the internet software piracy group, DrinkOrDie (US DoJ 2007f). The AHTCC has also been working collaboratively with overseas law enforcement agencies in identifying and investigating technology-enabled cases.

Framing appropriate charges

Police and prosecutors usually have some discretion with respect to the most appropriate charges that might be brought against suspects involved in technology-enabled crimes. Two types of difficulty can arise:

- the absence of appropriate offences in legislation
- the possibility that several charges may be appropriate which leads to choices having to be made between competing charges.

The first problem is exemplified by early cases in which no computer-related offence provisions existed to prosecute a suspect. For example, in the case of *R v Whiteley* [1991] 93 Cr App R 25, an early English hacking case, a defendant was prosecuted under the *Criminal Damage Act 1971* (UK) and was convicted on charges of damaging property. However, he appealed on the basis that unauthorised access to computer data did not itself constitute damage to tangible property – a requirement as the legislation defined property to mean property of a tangible nature. What had arguably been damaged, through the modification and erasure of some files, was information – but this is traditionally not classed as property for the purposes of offences such as theft or damage.

The appellate court in *R v Whiteley* carefully considered the arguments and applicable legislation, and was able to uphold the conviction on the basis that the statute required damage to tangible property, not that it required the damage itself to be tangible. In this case, there had been damage to tangible property (the disks) by way of unauthorised rearrangement of the magnetic particles on them, even though that might not have amounted to tangible damage. Moreover, it did not matter that the damage caused could only be perceived by operation of the computer to inspect the files, as opposed to physical inspection of the computer.

Similarly, in relation to the infamous Love Bug computer virus (or more accurately, virus/worm combination) which appeared in Hong Kong in 2000 and rapidly spread throughout the world's computer networks infecting both business and government computer networks, the problem of lack of appropriate offence provisions arose. Experts quickly identified the Philippines as the likely source of the code, and an investigation by the Philippines National Bureau of Investigation assisted by United States Federal Bureau of Investigation agents produced a suspect, a former computer science student. Warrants for a search of premises and computer equipment were executed, and enough evidence emerged for the suspect to be charged.

However, the prosecution encountered difficulties in selecting appropriate offences under Philippine law, as there was no existing offence of disseminating harmful computer viruses. The closest available offences involved theft and credit card fraud, but these were dismissed in subsequent legal proceedings as inapplicable and unfounded. Moreover, the double-criminality requirement for extradition was also not satisfied, meaning that the suspect could not be prosecuted in jurisdictions such as the United States which did have applicable computer crime laws.

Complicity in technology-enabled crimes

Complicity in technology-enabled crimes may arise in the following forms:

- aiding and abetting – active assistance or encouragement of a crime by a person who is physically present at its commission.
- counselling or procuring – active encouragement of a crime before it occurs.
- assisting escape or destroying evidence – acts after an offence has been committed which are intended to help the perpetrator avoid detection or capture.

All Australian jurisdictions have statutory provisions embodying these types of complicity, and the general rule is that an aider and abettor or other accessory may be punished as though a principal offender. Supplementing these provisions are common-law doctrines such as acting in concert, according to which two or more offenders who agree to commit a crime and are present at its commission are jointly liable as principals, and common purpose, which extends the scope of this liability to criminal acts which were not necessarily agreed at the outset but were foreseen as possible outcomes of the joint criminal enterprise. Even where an agreement to engage in criminal activity is not carried out or is prevented, those involved may be guilty of crimes of conspiracy (Bronitt & McSherry 2005).

The complicity provisions applicable to technology-enabled crimes prosecuted under Commonwealth laws are those contained in Part 2.4 of the *Criminal Code Act 1995* (Cth). In particular, s11.2 provides that a person who aids, abets, counsels or procures the commission of an offence by another person is taken to have committed that offence and is punishable accordingly. Subsection (2) provides:

> For the person to be guilty:
>
> (a) the person's conduct must have in fact aided, abetted, counselled or procured the commission of the offence by the other person; and
>
> (b) the offence must have been committed by the other person.

Subsection (3) provides:

> For the person to be guilty, the person must have intended that:
>
> (a) his or her conduct would aid, abet, counsel or procure the commission of any offence (including its fault elements) of the type the other person committed; or
>
> (b) his or her conduct would aid, abet, counsel or procure the commission of an offence and have been reckless about the commission of the offence (including its fault elements) that the other person in fact committed.

Numerous cases involving technology-enabled crime have involved multiple offenders and accessories, whether assisting before, during or after the event. Examples include groups of hackers, internet fraud scammers and child pornography rings (Smith, Grabosky & Urbas 2004). The most common examples of complicity in technology-enabled crimes generally arise in relation to the provision of hardware, software or expertise that assists in online criminality.

Examples of potential accessories to such crimes include:

- members of the public recruited to receive funds into their bank accounts before transferring the money overseas using wire transfer services, minus a certain commission payment and thereby facilitating money laundering (HTCB no. 16)

- business or government employees who disclose passwords, security codes, database details or personal information obtained from work computers/databases to others and thereby intentionally or recklessly facilitate unauthorised access
- software crackers who strip business or entertainment computer programs of their copyright and information management protections and distribute these through 'warez' websites
- providers of illegal signal decoding hardware or similar circumvention devices that allow users to obtain unauthorised free access to pay TV and similar subscription services
- creators and manipulators of malicious software (malware) such as viruses, worms, bots and spyware that can be used to steal confidential information or hijack computer functions in furtherance of financial or other crimes
- users of card skimming or similar devices that can surreptitiously capture personal and financial details and facilitate identity fraud and financial crimes
- computer experts in encryption, steganography or data removal that can assist in concealing criminal activities or removing evidence that may incriminate offenders
- members of hacker communities sharing security information that allows others to obtain unauthorised access to computers or data
- members of hacker communities building their own encrypted programs (e.g. CarderIM) to establish secure encrypted communication that facilitates them to sell confidential information (e.g. credit card numbers and email addresses), part of an underground economy dealing in financial data.

In all of these cases, those assisting may be liable for primary offences themselves as well as complicit in the crimes of other perpetrators. There are numerous statutory provisions that directly cover such acts as the supply of copyright-infringing software or circumvention devices (*Copyright Act 1968* (Cth), s132), using the internet to commit or facilitate other crimes (*Criminal Code Act 1995* (Cth), s474.14) and using a device to dishonestly obtain personal financial information (*Criminal Code Act 1995* (Cth), s480.5). Use of the internet to commit or facilitate sabotage or terrorist attacks is encompassed in the Criminal Code's definition of terrorist act in s100.1 (Urbas 2005). In addition, there are offences relating to terrorist organisations that may extend to website activities intended to promote or facilitate the activities of particular groups (*Criminal Code Act 1995* (Cth), s101.5, s102.4 and s102.7).

There are also recent provisions that impose obligations on internet service providers (ISPs) and internet content hosts (ICHs) to alert police about suspected online child pornography and child abuse material (*Criminal Code Act 1995* (Cth), s474.25), and enforcement powers to compel persons with knowledge of passwords or computer security protections to assist investigators (*Crimes Act 1914* (Cth), s3LA and *Customs Act 1901* (Cth), s201A). As organised crime groups move to greater use of the internet and other computer-related technologies, particularly in committing fraud and financial crimes, it can be expected that computer experts who assist by providing their tools of trade will face accessorial liability in relation to these activities. Highly skilled crackers in software piracy groups, for example, have been prosecuted for their role in criminal conspiracies to infringe copyright in the United States and other jurisdictions (US DoJ 2005).

The requirement that a person be physically present at a crime to be liable for aiding and abetting poses some conceptual difficulties in the online environment. The cross-jurisdictional reach of the internet has the consequence that persons located in Australia may, for example, be able to engage in online conduct that has effects on the other side of the world. In some cases, the legal doctrine of constructive presence may be used to explain how people may be liable for offences committed elsewhere, or it may be possible to connect them with an international conspiracy that extends beyond their particular physical location (US DoJ 2005). In some cases, it is conceivable that two or more offenders might be seen as jointly complicit or acting in concert online even if not physically located in the same place.

Recent arrests of participants in international child pornography rings, including some Australians, have produced evidence of the highly disturbing practice of live child sexual abuse video being streamed to internet chat rooms, with the actual perpetrator responding in real time to commands from other participants viewing the images (US DoJ 2006). Using a doctrine of constructive presence, it may be possible for such co-offenders to be prosecuted not only in relation to child pornography distribution, but also as accomplices in the sexual assaults. In some jurisdictions, there are offences of aggravated sexual assault in company (e.g. *Crimes Act 1900* (NSW), s61JA, with a penalty of imprisonment for life), that might be applicable to situations involving such groups of online perpetrators. However, these possibilities await prosecutorial consideration and legal exploration in Australian courts.

Defences and defence arguments

Defences may be either complete, in that if they are successful an acquittal follows, or partial, which if successful can only result in conviction for a lesser offence. Traditionally, a distinction is also made between justifications, being circumstances that render an act lawful that would otherwise be criminal, and excuses, which are circumstances peculiar to the accused person that may lessen culpability. Generally recognised defences include necessity, duress, provocation, self-defence, automatism, insanity and diminished responsibility (Bronitt & McSherry 2005).

Alongside these legal defences there is a range of defence arguments or strategies that may operate in a similar way. Thus, while intoxication is not strictly speaking a defence, the fact that a defendant was affected by alcohol or drugs at the time of committing an offence may negate the specific intent necessary for a particular crime, and so the result may be conviction for a lesser offence. The denial of an element of an offence or a challenge to the admissibility of certain evidence may also have a result similar to a successful defence.

Some cybercrime offence provisions incorporate specific defences that exclude liability for certain persons or situations. For example, internet child pornography offences (ss474.19 and ss474.20) and child abuse material offences (ss474.22 and ss474.23) in the *Criminal Code Act 1995* (Cth) are qualified by public benefit defences (ss474.21 and ss474.24) which are limited to law enforcement investigations and approved scientific, medical or educational research. Similarly, offences of using the internet or email to procure or groom persons under 16 years of age (ss474.26 and ss474.27) have a defence of belief that the person involved was not under 16 years (ss474.29). Given that many cybercrime offences are broadly drafted and carry substantial maximum penalties, such defences are a necessary protection against over-criminalisation.

More generally, those engaged in protecting computer networks from intrusion or defending their interests online may be able to raise general defences such as necessity or self-defence for unauthorised access to data or damage to computers. It is understood that reverse hacking (e.g. victims resorting to illegal hacking-back remedies) is sometimes committed in response to threats to data or computer security (Hutchinson & Warren 2001). Self-defence may extend to defence of property in some situations, so that owners of intellectual property might be able to raise such a defence where their response involves closing down pirate websites. Counter-measures to terrorist and other security threats may also involve action against website propaganda or networks used by potential offenders.

Some defence arguments specific to technology-enabled crimes have started to emerge, such as challenges to the admissibility of electronic evidence, assertions that computers were under the control of other parties (commonly known as the Trojan defence), and claims that online behaviour was merely role-playing. Defendants charged with technology-enabled crimes such as denial of service attacks have sometimes argued that their computer was infected with malicious software (malware) such as a bot malware that made it perform functions beyond their control and knowledge (Brenner, Carrier & Henninger 2004). To further substantiate their arguments, it is also possible for criminals to deliberately infect their computers with malware prior to committing the crimes, although it may be difficult to remove entirely evidence of this having occurred (Choo, Smith & McCusker 2007). Similar arguments have sometimes been raised when child pornography is discovered on personal computers. In some cases, these arguments may be without merit, but unless the prosecution can convincingly exclude the hypothesis of external infection beyond reasonable doubt, the defendant may be acquitted.

Another defence strategy is to challenge the legality of electronic searches conducted by law enforcement officers to obtain evidence of high tech crimes. Many jurisdictions require a search warrant based on reasonable suspicion of the existence of evidentiary material relevant to a crime before private premises can be searched, and this principle extends to contents of computers. Defendants can challenge the basis on which it was decided that a computer should be searched or seized, and similarly for the specific contents of the computer such as files, directories or records of internet activity. If the search is insufficiently related to the purposes for which the warrant was issued, this may raise a basis for excluding the evidence as improperly or illegally obtained.

Defendants might also challenge the presumption of reliability (presuming that computer forensic software such as EnCase reliably yields accurate digital evidence) particularly if open source forensic tools that have not been cross-validated (cross-checking the results of one software tool against the results of another based on industrial baselines) were used to extract the digital evidence.

> … The reliability of a particular computer system or process can be difficult to assessProgrammers are fallible and can unintentionally or purposefully embed errors in their applications. Also, complex systems can have unforeseen operating errors, occasionally resulting in data corruption or catastrophic crashes. Possibly because of these complexities, courts are not closely examining the reliability of computer systems or processes and are evaluating the reliability of digital evidence without considering error rates or uncertainty (Casey 2002).

Defence arguments raised in response to child pornography or child grooming prosecutions have included the fantasy defence, according to which the sender of messages to underage children claims to have really believed that the person with whom they were dealing was an adult, and that all concerned were merely role-playing or engaging in sexual fantasies (Smith, Grabosky & Urbas 2004). Of course, in some cases such a belief would be accurate, as a number of successful investigations in Australia and overseas have involved law enforcement officers posing as children online and engaging in chat room conversations with predators.

Although in some jurisdictions, the defence of entrapment might succeed in such situations if it can be argued that the defendant did not seek to engage in criminal activity but was merely enticed into doing so by a sting operation, the court might have little sympathy for the accused person as illustrated in the case of *R v Ferguson* [2006] 3 DCLR(NSW) 70 (9 March 2006). Ferguson responded to an advertisement posted by an undercover officer on the internet selling child pornography magazines offering to make videos with his stepdaughter, and write scripts for the same activity. Although no children were ever likely to be victimised in this case, Ferguson was sentenced to a term of two years and two months imprisonment with a non-parole period of one year and four months.

Some defendants have also argued, usually unsuccessfully, that engaging in such behaviour was therapeutic or was part of a research project (see Smith, Grabosky & Urbas). It was noted that:

> [i]ssues commonly introduced by the defense in undercover cases, such as entrapment, role-playing or fantasy, and the crime as a factual or legal impossibility, are common but seem to be ineffective (Mitchell, Wolak & Finkelhor 2005).

Seeking professional help (e.g. psychiatric or psychological treatment and counselling) has also been raised as an indication of remorse and a mitigating factor. For example, in the case of *R v Kennings* [2004]

QCA 162 (14 May 2004), the judge found the original sentence to be ‘manifestly excessive in all the circumstances, including the fact that no real child was the recipient of the applicant’s communications, the applicant’s remorse and cooperation with the authorities and his ongoing treatment and prognosis’.

Denial of improper purpose has also been a feature of some unauthorised access (hacking) cases, where it is claimed that the defendant was merely pursuing the altruistic aim of exposing the vulnerabilities of computer systems and databases (Smith, Grabosky & Urbas 2004).

Sentencing issues

Even where a person is convicted of the offence charged, a wide range of factors may be taken into account at sentencing to mitigate the penalty imposed. Mitigating factors generally may include a defendant’s youth, absence of prior offending, remorse or reparation, personal difficulties or financial circumstances, lack of malicious motive, presence of altruistic motive, absence of harm caused to victims, and so on. Even if a factor such as reduced mental capacity or lack of intent is insufficient for a defence, it may still be taken into account in mitigation of sentence (Fox & Freiberg 1999).

Recent studies by Kshetri (2006) and Jen, Chang & Chou (2006) indicated that a sizeable percentage of cybercriminals in Russia and Taiwan belong to the educated Y generation group (HTCB no. 13). Given the relatively young ages of some offenders, frequently advanced mitigating factors such as youth or lack of prior criminal offending arise often in cybercrime cases. Young offenders are also more likely to be considered capable of rehabilitation, so expressions of remorse or lack of malicious intent are readily accepted as mitigating the severity of punishment.

Addiction to computers (internet addiction) encompasses a wide-range of behaviours and impulse control problems. Young (1999) categorised computer addiction into cybersexual addiction, cyberporn, net compulsions (e.g. obsessive online gambling and shopping, information overload (e.g. excessive web surfing) and computer addiction (e.g. excessive online gaming). In some cases, claims of internet addiction disorder have been raised to explain particular forms of computer misuse such as hacking, and on occasions have been sympathetically received by sentencing courts. For example in the 1997 case involving Wandii’s trial, computer addiction was submitted by the defence with Wandii being acquitted of computer conspiracy charges by the jury (Dreyfus 1997).

Consideration of a significant number of sentences handed down for computer-related crimes in Australia and other countries reveals that there are certain recurring factors that affect sentencing (Smith, Grabosky & Urbas 2004). Mitigating factors include:

- good character or no previous convictions
- belief that conduct was/should be legal
- absence of harm to victim or public/personal gain to offender
- offender health problems including mental health
- addiction to computers or the internet
- prank – no malicious intent
- expression of genuine remorse
- cooperation with police investigation
- young age of offender
- repaid some or all of loss
- good prospects for rehabilitation

- had intended to alert victims to risks of computers.

By contrast, aggravating factors include:

- large financial loss or repair costs
- large number of counts or extent of illegality
- breach of government agency's security or computers
- prior convictions or repeat offender
- breach of trust as employee
- abhorrent crime (e.g. child pornography)
- victim company forced into liquidation
- offences committed while on parole
- environmental harm
- presence of special skills
- lack of remorse
- potential of harm to victims.

The review of cybercrime sentencing cases carried out by Smith, Grabosky & Urbas (2004) concluded by observing:

> Sentencing practices in cases of cyber crime are, however, continuing to develop, and arguably some sentences may seem overly lenient. Cyber crime is seen as a novel phenomenon, with some types of conduct only recently having been proscribed. On the other hand, courts have been required to emphasise the need for deterrence, and have actively made an example of those who break new laws….. Generally, it is the ability of those who misuse computers to inflict extensive damage upon multiple victims that makes these crimes so serious. The difficulty that courts face in sentencing is to impose an appropriate punishment that will have some deterrent effect while at the same time balancing the often compelling mitigating factors (Smith, Grabosky & Urbas 2004: 149).

5
Law enforcement and evidentiary issues

Law enforcement and technology-enabled crime

Law enforcement operates at three broad levels involving the prevention, investigation and prosecution of crime. Public agencies have a limited role in the prevention of technology-enabled crimes, in part because the design of the personal computer and the global adoption of the internet have largely been in the hands of private sector forces with less focus on security than on functionality. Accordingly, the burden of protection against misuse of technology has fallen largely on individual users. There is a flourishing industry of computer security products and services, such as anti-virus software, anti-malware software, anti-computer forensics software and devices, intrusion detection devices, intrusion prevention devices and encryption tools, servicing the increasing desire of individuals and businesses to protect themselves against computer-related threats.

Nonetheless, there is a significant public role in the regulation of telecommunications, the protection of critical infrastructure and the minimisation of opportunities for criminal misuse to spread to new areas of activity. At the policy level, a range of Australian government agencies have a role to play:

- Australian Security Intelligence Organisation
- Australian Secret Intelligence Service
- Office of National Assessments
- Attorney-General's Department
- Defence Signals Directorate (DSD) at the Department of Defence
- Department of Broadband, Communications and the Digital Economy (DBCDE)
- Department of Education, Employment and Workplace Relations (DEEWR)
- Department of Innovation, Industry, Science and Research (DIISR)
- Australian Communications and Media Authority (ACMA).

Various government initiatives bring together these public agencies and private sector entities in responding to technology-enabled crime and security threats. For example, the Trusted Information Security Network (TISN) overseen by the Attorney-General's Department comprises the above departments and several others, as well as business groups, with a focus on protecting critical infrastructure including telecommunications, transport, banking and finance.

Law enforcement agencies have also developed specialisations and organisational units directed at technology-enabled crime. For example, the AFP has recognised the area of Information and Communications Technology (ICT) as providing criminal opportunities (AFP website: e-crime):

> ICT impacts on law enforcement because of the way in which it can facilitate both lawful and unlawful activities. Information technology, and specifically networked communications, provide users with the capacity to conduct business or other affairs with speed and volume, over distance and at relatively low cost, with the option of remaining virtually anonymous if so desired.

Together with other police services in Australia, the AFP in 2000 developed an Electronic Crime Strategy with a focus on five key areas:

- prevention
- partnerships
- education and capability
- resources and capacity
- regulation and legislation.

The focus on partnerships, education and law enforcement capability was boosted in 2003 with the establishment of the AHTCC, hosted within the AFP and incorporating representatives of state and territory police, private industry and government departments. The stated role of the AHTCC is to:

- provide a national coordinated approach to combating serious, complex and multi-jurisdictional technology-enabled crimes, especially those beyond the capability of single jurisdictions
- assist in improving the capacity of all jurisdictions to deal with technology-enabled crime
- support efforts to protect the National Information Infrastructure (NII) comprising the information technology and communications, banking and finance, water, energy and utilities, transportation, mass gatherings, food, and emergency services sectors.

The functions of the AHTCC relating to this role are:

- coordination of technology-enabled crime matters between Australian law enforcement, federal government and international agencies
- investigation of serious and complex matters either by the AHTCC or through cooperation or referral to a partner agency
- intelligence services that contribute to a better understanding of the technology-enabled crime environment
- liaison with government agencies, industry groups, businesses and other organisations on technology-enabled crime matters, including technical, investigative, business and policy
- knowledge of technology-enabled crime issues such as preventative measures, best practice investigative tools and techniques, expert advice, training and education.

The AHTCC includes as a part of its operations the Joint Banking and Finance Sector Investigation team (JBFSIT), which consists of federal, state and territory police, as well as investigators from the major banks including the Commonwealth Bank, ANZ, National Australia Bank, Westpac and Suncorp Metway. The focus of JBFSIT is on technology-enabled financial crimes such as internet bank fraud, phishing and deceptive recruiting within the banking and finance sectors.

Collection, examination, analysis and reporting of electronic evidence

Law enforcement officers, usually assisted by trained computer forensic analysts with specialist skills in computer investigations, play a critical role in relation to electronic evidence. The strict evidentiary requirements for criminal prosecutions mean that there must be a demonstrable chain of custody in relation to any evidence collected, so that no reasonable doubt can be raised in relation to the authenticity and integrity of the data presented to court. to establish a chain of custody, organisations should ideally:

- create an evidence copy of an electronic record. Such copies can be created by various means including reproducing the electronic record as a printed document or copying the electronic record to storage media (e.g. backup tape).
- maintain a custody log of the evidence copy, recording details such as who accessed the evidence, when the evidence was accessed and returned (if evidence was removed) and why the evidence was accessed.

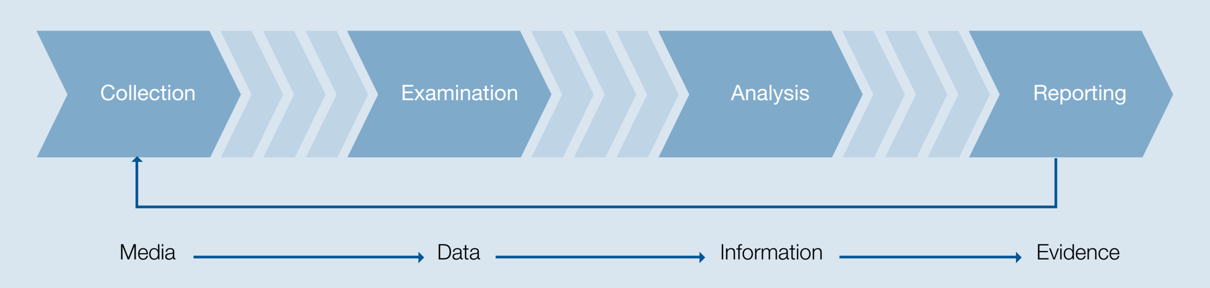
In particular, verification is needed that the contents of a computer have not been created, deleted or modified during search, seizure and subsequent analysis. In this regard, it is critical that the analysis be undertaken by appropriately trained and skilled computer forensic analysts (the process of forensic copying is described further below).

Digital evidence differs from traditional evidence. The former is intangible and often transient in nature, and can easily be duplicated, copied, shared, disseminated, modified and damaged. A recent case involving Jim Selim of the now-defunct Pan Pharmaceuticals (SMH 2007) is an indication of how easily electronic data can be destroyed to prevent investigators from acquiring digital evidence.

To address the specific and articulated needs of law enforcement and to ensure (digital) evidentiary admissibility, computer forensic researchers and practitioners have developed various models for the computer forensic process. Computer forensics can be defined as the science of identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data (NIST 2006a).

Although models for the computer forensic process differ primarily in how granular each phase of the process is and in the terms used for specific phases, they reflect the same basic principles and the same overall methodology (NIST 2006b) particularly proper documentations for the chain of custody. The basic model adopted by NIST (2006b) is described in Figure 2.

Figure 2: A basic computer forensic process



Source: NIST (2006a): 3-1

- Collection – The identification of digital evidence is typically the first step in the forensic processes for computer forensic models. Knowing what evidence is present, where it is stored and how it is stored is vital to determining which processes are to be employed to facilitate its recovery. Computer forensic examiners must be able to identify the type of information stored in a device and the format in which it is stored so that the appropriate technology can be used to extract it.
- Examination – Given the likelihood of judicial scrutiny in a court of law, it is imperative that any examination of the electronically stored data be carried out in the least intrusive manner. There are circumstances where changes to data are unavoidable, but it is important that the least amount of change occurs. In situations where change is inevitable it is essential that the nature of, and reason for, the change can be explained.
- Analysis – The analysis of digital evidence includes the extraction, processing and interpretation of digital data. This is generally regarded as the main element of forensic computing. Analyses should be performed on the evidence copy and care taken not to alter the original copy of the evidence. Once extracted, digital evidence usually requires processing before people can read it.
- Reporting – The presentation of digital evidence involves the actual presentation in a court of law. This includes the manner of presentation, the expertise and qualifications of the presenter and the credibility of the processes employed to produce the evidence being tendered.

Accreditation of computer forensic examiners and forensic laboratories and validation of computer forensic tools

Increasingly, forensic analysis of computers for law enforcement purposes is being undertaken by well-organised groups of computer forensic examiners working in government facilities or private sector workplaces such as leading consulting practices. Only specially trained and authorised computer forensic examiners should process and examine electronic evidence, as evidence not retrieved by a computer forensic expert may result in the reliability of the evidence itself being called into question and potentially being ruled inadmissible in court. To ensure that the results of computer forensic examinations can be used in judicial proceedings, accreditation of individual examiners (see Table 5) and validation of computer forensic analysis tools is desirable.

Accreditation of computer forensic examiners

In Australia, there is neither a formal accreditation system for computer forensic examiners nor a requirement for expert witnesses to be members of professional societies (e.g. Australian Computer Society, Engineers Australia and National Institute of Forensic Science). There are, however, plans for a formal accreditation system for computer forensic examiners to be introduced shortly under the auspices of the National Accreditation of Testing Authorities (NATA).

Having a national accreditation program for expert witnesses in computer forensics would assist the courts in testing the qualifications of expert witnesses, although they would still be subject to cross-examination regarding their expertise in any given case. There are parallels here with the sometimes contentious introduction of other forensic techniques such as DNA profiling, facial imaging and other biometric techniques that are now generally accepted as useful sources of evidence in Australian courts.

Accreditation may help to avoid situations such as that which occurred in the United States where a so-called computer forensics expert hired to testify at two child pornography court cases pleaded guilty to federal perjury charges for falsifying his resumé and lying in open court, presumably about his credentials (Goodin 2007, US DoJ 2007a). The indictment alleged that '[a]t the time Edmiston worked on the child porn cases, he had already been qualified as an expert witness in computers and submitted court testimony in several jurisdictions, including the federal court in California, and in courts in at least two California counties'.

Table 5: Examples of computer forensic certification organisations

Certifications	Organisation (Website)
Certified Computer Examiner (CCE)	International Society of Forensic Computer Examiners (http://www.isfce.com/)
Certified Forensic Computer Examiner (CFCE)	International Association of Computer Investigative Specialists (http://www.iacis.com/iacisv2/pages/home.php)
Computer Analysis Response Team (CART) Program	United States Federal Bureau of Investigation (http://www.fbi.gov/hq/lab/org/cart.htm)
CyberSecurity Forensic Analyst (CSFA)	CyberSecurity Institute (http://www.cybersecurityinstitute.biz/)
GIAC Certified Forensics Analyst (GCFA)	SANS Institute (https://www.sans.org/)

Validation of computer forensic tools

In the United States in December 2005, the Computer Forensic Tool Testing (CFTT) project was established, supported by the United States Department of Justice's National Institute of Justice (NIJ), federal, state, and local law enforcement, and the National Institute of Standards and Technology (NIST). The goal of the CFTT project was to 'establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools capabilities' (see http://www.cftt.nist.gov).

To reduce the risk of computer forensic evidence being called into question in judicial proceedings, only validated forensic analysis tools (e.g. EnCase software) that have been accepted by courts in Australia and other common-law jurisdictions should be used to gather and analyse evidence.

The importance of carrying out forensic examinations of hard drives carefully is demonstrated in the case of Peach v Bird 159 A Crim R 416 [2006] NTSC 14 (21 February 2006). In that case, the defendant had been acquitted of charges of possessing child pornographic images. An appeal under s163(3) of the *Justices Act 1928* (NT) was lodged. Although no images of child pornography were able to be recovered from the hard drive, the forensic examiner, using EnCase software found various incriminating file names as well as evidence that the hard drive had been erased and overwritten in an attempt to remove evidence. The forensic examiner reported that:

> [T]he hard drive of the computer contained a word document named 'untitled document.wps' ('the untitled word document'). The document was found in the computer folder, C:\\My Documents. The word document contained a number of links to or addresses of websites, including the link, 'http://mx.photos.yahoo.com/pishanito2002' (the pishanito website). The hard drive of the computer also contained a directory of 70 images and one temporary storage file of a word document that had been stored in the C:\\My Documents\\My Pictures folder of the computer. The 70 images and the one word document contained in the directory had been overwritten or erased with the use of eraser programs on the computer. This meant that the 71 files could no longer be recovered. All that could be seen was the name of each file that had been saved to the C:\\My Documents\\My Pictures folder of the hard drive; the date that each file was created and the date that each file was overwritten or erased. Unlike a file which has been merely deleted, a file which has been overwritten or erased cannot be recovered. The erasing programs on the computer had been run on the files/images rather than the whole of the folder including the directory of file names of the 70 images and one word document. One of the files of the 70 erased images in the directory was named 8087053lg0.jpg. A jpg file is an image or picture file as opposed to a text file. The file named 8087053lg0.jpg was created on 17 March 2003 and overwritten or erased on 18 March 2003.

Based on this evidence, the acquittal was set aside and a retrial ordered. On 28 August 2006, an appeal was also dismissed (see *Bird v Peach* [2006] NTCA 7 (28 August 2006)).

Accreditation of computer forensic laboratories

Unlike other disciplines, accreditation of computer forensics laboratories is not currently included in the 16 categories of accreditation for facilities and laboratories by NATA in Australia. In the United States, accreditation of computer forensics laboratories was included by the American Society of Crime Lab Directors, Laboratory Accreditation Board (ASCLD-LAB) in 2005. The United States Defense Computer Forensics Lab (DCFL) was the first such laboratory to be accredited by ASCLD-LAB in recognition of 'the DCFL's rigorous and reliable processes and ability to successfully meet the growing demands of cyber crime prevention' (USAF 2005). To further strengthen law enforcement's computer forensic capabilities throughout the United States, the Regional Computer Forensics Laboratory (RCFL) program supporting the ASCLD/LAB accreditation was established by FBI's Operational Technology Division (OTD). Adopting a similar approach of accreditation for computer forensics laboratories in Australia (e.g. AS ISO/IEC 17025-2005 accreditation and the equivalent of the RCFL program accredited by ASCLD/LAB) will be an important step in the evolution of the discipline.

Search and seizure powers

The *Crimes Act 1914* (Cth) contains various provisions concerning search and seizure of evidence in federal criminal matters. There are specific provisions relating to electronic searches, including powers to bring equipment such as laptops with forensic imaging programs to specified premises (s3K) and to use electronic equipment found at premises such as computers and printers (s3L).

Section 3LA of the *Crimes Act 1914* (Cth) and s201A of the *Customs Act 1901* (Cth) make it an offence for persons with knowledge of computers or computer networks of which computers form a part, or measures applied to protect data held in, or accessible from, computers, to fail to provide any information or assistance that is reasonable and necessary to allow access to data held in, or accessible from, a computer that is on warrant premises, to copy the data to a data storage device, or to convert the data into documentary form. Failure to comply carries a maximum penalty of six months imprisonment. These are important provisions designed to overcome the efforts of accused persons to conceal data through the use of passwords or encryption.

Where there are defects with warrants, or the search conducted exceeds the scope of the warrant, a defendant may seek to have the evidence obtained as a result of the search ruled inadmissible under s138 of the *Evidence Act 1995* (Cth). It is therefore important to ensure that warrants are properly drafted, obtained and executed for the results of searches to be admitted into evidence.

Subsection 3E(1) of the *Crimes Act 1914* (Cth) provides that:

> An issuing officer may issue a warrant to search premises if the officer is satisfied by information on oath that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential material at the premises.

The warrant must state a number of listed matters, including 'the kinds of evidential material that are to be searched for under the warrant' (s3E(5(c)). The term evidential material is defined to mean 'a thing relevant to an indictable offence or a thing relevant to a summary offence, including such a thing in electronic form' (s3C). Thus, the contents of computers or other electronic storage devices may be searched under warrants.

Evidential material may be seized if it is specified in the warrant or if the executing officer believes on reasonable grounds that it is evidential material in relation to the offence to which the warrant relates or another indictable offence (s3F). Thus, computers and electronic devices may be seized, but only if they have been sufficiently examined for the requisite belief to be formed.

Division 2 of the *Crimes Act 1914* (Cth) imposes certain limitations on the ability of investigators to conduct in depth searches of computers to examine their contents. For example, data examination involves assessing and extracting the relevant pieces of information from the collected data. The latter is by no means easy due to increased data storage capacities. An acquired storage medium is likely to contain hundreds of thousands of data files. Identification of data files containing information of interest is both time consuming and be daunting. Moreover, identified data files of interest may contain extraneous information that needs to be filtered. With the advent of more complex data storage and dissemination technologies, computer forensic examiners face an increasingly difficult task. Developments in data storage and dissemination technologies can impede computer forensic examiners and prevent police from acquiring digital evidence and analysing digital content forensically within the time-frame specified in the Act. In particular, section 3L(6) provides that computer equipment can only be held for up to 24 hours unless an application is made for an extension. The use of data copying techniques, however, make this period of time generally sufficient for copying data, although considerably longer periods are needed for analysis of the copied data.

There is a danger that, unless searches are able to be carried out methodically, the contents of files may be deleted or altered. Therefore, a number of special provisions were added to the *Crimes Act 1914* by the *Cybercrime Act 2001* (Cth), facilitating computer searches. These are found in ss3L – 3LB (analogous provisions were introduced into the *Customs Act 1901* (Cth) by the *Cybercrime Act*, and there is a similar provision to s3LA also in the *Telecommunications Act* 1997 (Cth) relating to spam investigations.

Subsection s3K(1) of the *Crimes Act* provides that the executing officer may 'bring to the warrant premises any equipment reasonably necessary for the examination or processing of a thing found at the premises to determine whether it is a thing that may be seized under the warrant'. Subsection (2) provides that a thing found at the warrant premises 'may be moved to another place for examination or processing to determine whether it may be seized under a warrant' if the owner of the premises consent in writing, or if two conditions are satisfied:

(i) it is significantly more practicable to do so having regard to the timeliness and cost of examining or processing the thing at another place and the availability of expert assistance; and

(ii) there are reasonable grounds to believe that the thing contains or constitutes evidential material.

There are notice requirements under subsection (4), and a time limit of 72 hours applies to the examination process under subsection (ss3K(3A)), extendible if 'the executing officer believes on reasonable grounds that the thing cannot be examined or processed within 72 hours or that time as previously extended' (ss3K(3B). Subsection (4) provides that the executing officer 'may operate equipment already at the warrant premises to carry out the examination or processing of a thing found at the premises to determine whether it is a thing that may be seized under the warrant if the executing officer or constable believes on reasonable grounds that:

(a) the equipment is suitable for the examination or processing; and

(b) the examination or processing can be carried out without damage to the equipment or the thing.'

Section 3L further provides that equipment found at warrant premises may be operated (subject to the similar conditions as in s3K(4) above) 'to access data (including data not held at the premises)'. This is potentially a powerful provision in that it may allow remote searches of computers connected via a network (possibly even across jurisdictional boundaries). The term data is defined to include information in any form and any program (or part of a program). The data may be copied to a disk, tape or other associated device (whether brought to the premises or, with consent, found on the premises) under s3L(1A). If data on premises other than warrant premises are accessed, there are obligations to notify the owner of those premises as soon as practicable (s3LB).

Finally, s3LA provides a power to compel, by order of a magistrate, any person suspected of having committed offences to which the warrant relates, or the owner or lessee of the computer or an employee of such a person, to provide assistance that is reasonable and necessary to allow the officer to do one or more of the following:

(a) access data held in, or accessible from, a computer that is on warrant premises

(b) copy the data to a data storage device

(c) convert the data into documentary form.

Failure to comply with such an order is punishable by up to six months imprisonment. The scope of this provision has yet to be tested in the courts, but is arguably of wide scope and application, which has created a degree of apprehension among some legal and computer professionals (see James 2004).

Although not all Australian jurisdictions have a specific warrant for the search and seizure of electronic evidence, existing legislation and procedures allow members of state and territory police services to apply to an authorised officer for search warrants to search the premises and to seize any such thing if found, and to take it before a justice to be dealt with according to law (see Table 6).

Table 6: Summary of main Australian search and seizure legislation applicable to electronic searches

	Provisions
Cth	*Crimes Act 1914*, s3E – 3F and 3K – 3LB *Customs Act 1901*, s198 – 199 and s200 – 201B
ACT	*Crimes Act 1900*, s200 (Use of electronic equipment at premises)
NSW	*Law Enforcement (Powers and Responsibilities) Act 2002*, s47 (Power to apply for warrant for particular offences) and s49 (Seizure of things pursuant to warrant)
NT	*Police Administration Act*, s117 (Search warrants) and s119 (Searches and emergencies)
Qld	*Police Powers and Responsibilities Act 2000*, s150 (Search warrant application) and s154 (Order in search warrant about information necessary to access information stored electronically)
SA	*Summary Offences Act 1953*, s67 (General search warrants) and s68 (Power to search suspected vehicles, vessels, and persons)
Tas	*Search Warrants Act 1997*, s11 (Use of electronic equipment at premises)
Vic	*Crimes Act 1958*, s465 (Issue of search warrant by magistrate), s86VB (Power to enter public authority premises) and s86VC (Power to seize documents or things at public authority premises)
WA	*Criminal Code*, s711 (Search warrant)

Source: Compiled from legislative databases including http://www.comlaw.gov.au/, http://www.legislation.act.gov.au/, http://www.legislation.nsw.gov.au/, http://www.nt.gov.au/dcm/legislation/current.html, http://www.legislation.qld.gov.au/OQPChome.htm and http://www.austlii.edu.au/

In addition, Division 4 of the *Telecommunications Act 1997* (Cth) – amended by the *Spam (Consequential Amendments) Act 2003* (Cth) – provides inspectors (as defined by *Telecommunications Act 1997* (Cth), Section 533) with powers to enter and search premises if a breach of the *Spam Act 2003* (Cth) is suspected.

It is also likely that during the course of an investigation, sources of evidence may be identified which are located overseas. Examples arise in botnet-related cases where infected computers – zombie computers – used to launch distributed denial-of-service attacks are located in other countries. In such cases, the relevant country should be contacted for assistance by means such as the 24/7 network of contacts hosted by the AHTCC (see section 'Cross-border cooperation').

Cases on search and seizure provisions

The search and seizure provisions of the *Crimes Act 1914* (Cth) have been considered in a number of cases involving computer searches. The first case to examine the question of the seizure of computer equipment was *Bartlett v Weir and Ors* (1994) 72 A Crim R 511. In that case, police seized computer equipment to examine floppy disks named in the warrant. The presiding judge decided that the execution of the warrant in the case was unlawful for the following reasons.

> …. consider that the execution of the warrant in its entirety was fundamentally flawed for the reasons which I have stated, namely, that the second respondents seized items without knowing whether they fell within the terms of the warrant, intending to examine them later, and without having held, at the time of seizure, the requisite reasonable belief that the goods seized might afford evidence of the commission of a crime. Accordingly, I am of the opinion that the execution of the warrant at … was unlawful.
>
> I am of the same opinion in relation to the seizure of items from the applicant's home…. There was no consideration of the content of the computer files which were seized at those premises at the time of execution of the warrant. In those circumstances, there could have been no reasonable basis for the second respondents to reasonably believe, in respect of each item seized, that it would afford evidence of the commission of the offences specified in the warrant or of any other offence.

In *Hart v Commissioner, AFP* [2002] FCAFC 392 (5 December 2002), the Federal Court found that s3K(2) did not authorise AFP officers to copy computer files to storage devices brought to the premises and then to move these devices to another place for analysis. This was because s3K in its terms allows things to be brought to premises for the purposes of analysis, and it allows things found at premises to be seized and taken away, but it does not explicitly allow things brought to the premises to be used to download evidential material and then taken away again for analysis. This drafting imposes a significant limitation on how searches may be conducted if relying on s3K.

Of course, s3L does enable copying of data onto devices which may be taken away, and it was held in the case of *Kennedy v Baker* [2004] FCA 562 (6 May 2004). The later case of *ASIC v Rich* [2005] NSWSC 62 (16 February 2005) confirmed that this constitutes seizure of the data for the purposes of s3F warrants, as (per Austin J at [238]):

> [I]n the case of evidential material which is an electronic thing, there is seizure of the electronic copy of the electronic thing through removal of the storage device after the downloading or copying is completed, regardless of whether the storage device is brought to the premises or found there, and regardless of whether it is used with or without the occupier's consent.

These cases raise the practical question of whether searches that purport to rely on one of the provisions in the Crimes Act, in particular as between s3K and s3L, preclude reliance on another. In a recent case, it was held that no such limitation is imposed by the legislation, and that 'there is nothing in the Act to suggest that the availability of one option precludes the choice of another': *Egglishaw v Australian Crime Commission* [2006] FCA 819 (30 June 2006).

It should be noted that agreement can be reached between investigating officers and other parties, in relation to the way in which computers (whether at warrant premises or removed) will be forensically examined. This may include restrictions on the material to be examined, such as those in which claims of legal professional privilege is claimed, and such agreements may be enforceable by the court: *Oke v Commissioner of the AFP* [2005] FCA 1363 (20 September 2005).

In general, drafting and executing of search warrants that relate to the search and seizure of digital evidence are similar to other investigations. Issues to be considered include:

- the criminal offence being investigated (e.g. possession and distribution of child pornography material)
- the venue of the search (e.g. physical address)
- the types of evidence expected to be found (e.g. computers and storage devices)
- the relevance of the evidence to the criminal offence (e.g. instrumentality of the crime).

A recent case that illustrates problems concerning the drafting and execution of search warrants in relation to computers and their contents, and how they may be challenged by the defence, was *R v PJ* [2006] ACTSC 37 (2 May 2006). In this case, a search warrant was obtained by the AFP in relation to a house in the ACT that was believed might contain evidence relating to the possession of child pornography. Information had been received by the AHTCC from an overseas country's law enforcement agency, identifying a phone number as having been involved in downloading child pornography material, and a list of names of files had been forwarded to the AFP's Sexual Assault and Child Protection Unit. The names on the list indicated that they referred to sexual activity involving young children. The warrant that was obtained authorised AFP officers to enter the premises and search for and seize evidential material, described thus:

> First Condition:
>
> Things which are:
>
> (a) video cameras, cameras, photographs video tapes, film, undeveloped film, paper, documents or anything else containing pornographic or sexually implicit or explicit images any child or underage person.
>
> (b) any and all computer equipment or other electronic storage devices capable of storing electronic data regarding above items, including magnetic tapes, floppy discs, hard drives, viewing screens, disc

> or tape drives, central processing units, printers, and all software necessary to retrieve electronic date, including operating systems, database, spreadsheet, work processing and graphics programs, all manuals for operation of computer and software together with all handwritten notes or printed confidential password lists to enter secured files. Also any printouts throughout location or trash re above items.
>
> Second Condition:
>
> Things which relate to any one or more of the following:
>
> (a) [full name of accused] born [correct date of birth]
>
> (b) [correct street and suburb]
>
> (c) any bills or correspondence from [stated telecommunications service provider] for the telephone number [stated correct number].
>
> Third Condition:
>
> Things as to which there are reasonable grounds for suspecting that they will afford evidence as to the commission of the following offences(s) against the laws of the Australian Capital Territory:
>
> (a) possession of child pornography contrary to section 65 of the Crimes Act 1900 (ACT).

The search that was conducted pursuant to the warrant involved a forced entry to the house, which was unoccupied at the time, and the analysis of the contents of a computer found inside. Sexually explicit images were revealed on the computer during this analysis, which was confirmed afterwards when the computer was removed from the premises and forensically imaged and examined at the AFP's computer laboratory. The search further uncovered videotapes in a locked cupboard in the garage, which was also found to contain a bag with computer disks. These were also examined later, and were found to contain sexually explicit images, which were also the subject of a charge of possessing child pornography under s65 of the *Crimes Act 1900* (ACT). At trial, the defence sought to have the evidence excluded on a number of grounds, all of which failed, including:

- irregularities in the search warrant (which had transposed the block and section numbers of the premises)
- execution of the warrant (as items such as the computer disks were seized without it having first been established that they contained evidential material)
- admissibility of a record of interview (conducted after the search and seizure of the defendant's premises).

Mr Justice Connolly of the ACT Supreme Court referred to the application of the *Human Rights Act 2004* (ACT) to the case. While acknowledging that the latter statute may have a bearing on the interpretation of legislation authorising search and seizure (such as the Crimes Act provisions under which the warrant was obtained), this in fact made little difference in terms of admissibility. The main reason is that the Human Rights Act defines as human rights (s5) those rights recognised under the International Convention on Civil and Political Rights (ICCPR). However, ICCPR rights are already to be taken into account under s138(3)(f) of the *Evidence Act 1995* (Cth), which applies in federal and ACT courts, in assessing whether evidence has been illegally or improperly obtained.

Forensic copying

The process of copying of evidence in a forensically sound manner is a fundamental element of the forensic computing process. The evidence (data) can be acquired from device using either physical acquisition or logical acquisition.

- Physical acquisition – A bit-by-bit copy of an entire physical storage device and allows deleted files and any data remnants present in the storage devices such as unused file system space to be examined.
- Logical acquisition – A bit-by-bit copy of the logical storage objects such as directories and files residing on a logical store (e.g. a file system partition).

Electronic data held on computer hard disks and digital media are very volatile forms of evidence. This evidence can be easily altered or destroyed if left unprotected or without proper handling. As in the case of traditional evidence, the proponent of evidence normally carries the burden of offering sufficient support to authenticate electronic evidence. A mechanism therefore to preserve or reproduce the data in a non-volatile format is required. Physical acquisition (disk imaging) allows an entire hard disk drive to be reproduced or analysed without the need to access the original hard disk. This process provides a safe mechanism to analyse, test and interact with data, while still providing the most accurate reproduction of the original. In this case the data copied can be said to be an exact duplication of the original, a more exact duplication than, for example, a photocopy of a page, as a disk image allows the recovery of deleted and ambient data.

Computer forensic examiners frequently use a number of methods to ensure the validity of the data copied including creating a digital signature (called a mathematical hash) of the data as it is read from the hard disk drive so that the signature can be compared to the copied data. The mathematical hashing algorithm (e.g. MD5 and SHA-1) allows an examiner to detect if data have been altered or an error has occurred in the copy process. A number of commercial forensic acquisition products even embed the mathematical hash into an electronic container that holds the forensic image.

In the case where only a file or files are copied (logical acquisition), as opposed to a copy of the entire hard disk (physical acquisition), a similar digital signature processes is applied. In such cases a mathematical hash of each individual file is created of the original at the time of copying.

The advantage of this copying and digital signature process is that it allows for multiple exact duplicates of data to be reproduced and certified (verified). These processes are used by law enforcement and commercial forensic computing providers.

The process of interacting with a computer subject to a judicial process can irreversibly damage data, even turning a computer on can subsequently alter many of the files that may be useful in the forensic examination. To this end examiners will employ some specific write-protection devices, either hardware or software that will eliminate the inadvertent or deliberate alteration of data on a computer hard disk drive. This process is essential if the original evidence needs to be interacted with in some way, such as producing a forensic copy, or performing a preview of the data to determine reasonable grounds to believe a thing (the computer) will afford evidence in the investigation.

Computer forensic analyst reports

The results of forensic analysis are routinely set out in a report prepared by the computer forensic analyst. This should state the nature of all examinations conducted, the personnel involved, and the basis for decisions made as to the relevance of material found. There is no standard form required for such reports to be tendered, and admissible, in Australian courts. Although requirements for such reports differ in jurisdictions, the expert witness code of conduct is adopted in most states and territories. For example, in the Supreme Court of NSW, the expert witness code of conduct in Schedule 7 of the Uniform Civil Procedure Rules 2005 under the *Civil Procedure Act 2005* (NSW) requires the following details to be included either in the body of the report or in an annexure:

- the expert's qualifications as an expert on the issue the subject of the report
- the facts, and assumptions of fact, on which the opinions in the report are based (a letter of instructions may be annexed)
- the expert's reasons for each opinion expressed, if applicable, that a particular issue falls outside the expert's field of expertise
- any literature or other materials utilised in support of the opinions
- any examinations, tests or other investigations on which the expert has relied, including details of the qualifications of the person who carried them out
- in the case of a report that is lengthy or complex, a brief summary of the report (to be located at the beginning of the report).

Similar expert witness code of conduct guideline is also adopted by the Federal Court of Australia (e.g. see Black 2007).

In general, the writer of the report will be called to give evidence in any contested proceeding in which the contents of the report are adduced as evidence. In addition to a computer forensic analyst's written report and testimony, evidence from computers may be tendered directly as documentary evidence. The requirements for documentary evidence, and for witnesses giving expert opinion evidence, are discussed below.

Evidentiary rules and presumptions

The law of evidence contains a number of rules and presumptions that may facilitate the admission of electronic evidence. Although both the *Evidence Act 1995* (NSW) and the *Evidence Act 2001* (Tas) mirror the *Evidence Act 1995* (Cth), there are some differences between these Acts (ALRC 2005). Evidence Acts based on the Commonwealth Act (known as the uniform Evidence Acts) apply to all proceedings in federal courts, or courts of the Australian Capital Territory, New South Wales and Tasmania. By virtue of section 79 of the *Judiciary Act 1903* (Cth), proceedings in state and territory courts will be governed by the relevant state and territory evidence Act and the applicable rules of court:

- *Evidence Act 1995* in New South Wales
- *Evidence Act* in the Northern Territory
- *Evidence Act 1977* in Queensland
- *Evidence Act 1929* in South Australia
- *Evidence Act 2001* in Tasmania
- *Evidence Act 1958* in Victoria
- *Evidence Act 1906* in Western Australia

There are, however, some miscellaneous provisions in the *Evidence Act 1995* (Cth) that apply in all courts within Australia. The following discussion briefly describes a selection of these as contained in the *Evidence Act 1995* (Cth), which applies in all federal courts and courts of the Australian Capital Territory.

Electronic Documents

Part 2.2 of the *Evidence Act 1995* (Cth) deals with documentary evidence, which includes evidence in electronic form since the definition of document in the Dictionary to the Act defines the term so as to include 'anything from which sounds, images or writings can be reproduced with or without the aid of anything else' (in conformity with the *Acts Interpretation Act 1901* (Cth)). Section 48 allows a party to proceedings to tender as proof of the contents of a document, among other things:

- the document itself
- a copy produced by a device that reproduces the contents of documents (such as a photocopier)
- 'if the document in question is an article or thing on or in which information is stored in such a way that it cannot be used by the court unless a device is used to retrieve, produce or collate it—tendering a document that was or purports to have been produced by use of the device' (ss48(1)(d))
- a document that 'forms part of the records of or kept by business (whether or not the business is still in existence)' (ss48(1)(e)).

Thus, a computer printout may be tendered as evidence of the contents of a computer file, a fax printout may be tendered as evidence of the contents of a faxed letter, and so on. For complex or voluminous documents, the court may direct that a summary be produced (s51), and the original document rule under common law (which restricted the admissibility of copies) is abolished (s51).

The operation of ss48(1)(d) and (e) in relation to the tender of a printed copy of an Excel spreadsheet in civil proceedings was considered in *Edmunds-Jones Pty Ltd v Australian Women's Hockey Association Inc* [1999] NSWSC 285 (19 March 1999), at [12] – [14], where it was considered that the provisions covered the tender of an edited version of the document where only formatting and deletion of irrelevant material were involved in preparation of the document (though the point was decided by invoking s190, allowing waiver of the rules of evidence).

In addition, there are provisions in Part 4.3 of the *Evidence Act 1995* (Cth) that facilitate the admission of electronic evidence by embodying presumptions as to the operation of processes, machines and other devices. Section 146 provides that, where a party tenders a document or thing produced by a device or process, then '[i]f it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document or thing on the occasion in question, the device or process produced that outcome'. The note to s146 gives the following example: 'It would not be necessary to call evidence to prove that a photocopier normally produced complete copies of documents and that it was working properly when it was used to photocopy a particular document'.

Section 147 of the *Evidence Act 1995* (Cth) is in similar terms, but relates to documents which are part of business records (whether or not the business is still in existence), and it provides that 'it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document on the occasion in question, the device or process produced that outcome'. The only difference from the s146 wording is that the reasonably open precondition is omitted.

Sections 146 and/or 147 have been applied in a range of cases in which the admissibility of certain documents was considered – for example, in relation to computer-generated vehicle journey reports (*Roads and Traffic Authority of New South Wales v Tetley* [2004] NSWSC 925 (8 October 2004)), automated teller machine records (*R v Magoulias* [2003] NSWCCA 143 (26 May 2003)), and bank statements (*ASIC v Rich* [2005] NSWSC 417 (5 May 2005)).

It is important to observe, however, that additional testimony will usually be needed to authenticate the document as coming from the source claimed (*National Australia Bank Ltd v Rusu* (1999) 47 NSWLR 309) – though note that the Evidence Act does allow a court to draw any reasonable inference from a document or thing, ‘including an inference as to its authenticity or identity’ (s58, and see also s183). In *ASIC v Rich* [2005] NSWSC 417, at [120], Austin J explained how the court would be able to draw inferences as to the source and identity of a computer-generated document using the *Evidence Act* provisions:

> If, hypothetically, ASIC tenders a document which on its face, purports to be a budget for the One.Tel Group for 2001, and adduces provenance evidence showing that the document was printed out from a computer hard-drive copied by the liquidators from One.Tel’s hard-drive, and establishes a file path through the finance directory to a subfile called Budget 2001, the court would be able to conclude on the balance of probabilities (see s142) that the document had been adequately authenticated. Such evidence does not show who created the document (although the properties page, if in evidence, might assist in that respect), or how the document was used within the organisation, or even whether it is the only version or might have been a draft. But it is sufficiently well authenticated to be received, provided it is properly tendered under s48 and is admissible. There is evidence, not confined to inferences from the document itself, showing on the balance of probabilities (see s142) that the document came from One.Tel’s financial records where it was classified as a 2001 budget, which is what it purports to be.

Other provisions in Part 4.3 of the Act facilitate proof of the contents of postal articles (s160), telexes (s161), lettergrams and telegrams (s162) and letters sent by Commonwealth agencies (s163). In general, there is extended application of provisions relating to documents where these are or were part of Commonwealth records (s182).

Relevance and exclusionary rules

In order to be admissible, evidence about the contents of documents (whether electronic or otherwise) must be relevant and not excluded by any of the remaining evidentiary rules (such as the hearsay, opinion, or tendency and coincidence rules), by the claim of legal or other forms of privilege, or by the exercise of judicial discretion to exclude (due to unfair prejudice, or impropriety and/or illegality). In general, the hearsay rule does not apply to output that is generated automatically by the computer following previously programmed instructions without further human intervention and data independently recorded by a computer without significant human involvement. For example, Section 95 of the *Evidence Act 1929* (Qld) provides an exception to the hearsay rule for statements produced by computers where:

- that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not, by any person (see ss95(2)(a))
- that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived (see ss95(2)(b))
- that throughout the material part of that period the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents (see ss95(2)(c))
- the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities (see ss95(2)(d)).

The key requirement for admissibility is *relevance*, either to facts in issue or at least to the credibility of a witness (s55). Therefore, any (electronic or other) evidence will be excluded as inadmissible if not relevant in a proceeding (s56). The Evidence Act defines evidence which is relevant in a proceeding as ‘evidence that, if it were accepted, could rationally affect (directly or indirectly) the assessment of the probability of the existence of a fact in issue in the proceeding’ (s55(1)). Evidence may also be admitted as provisionally relevant (s57).

An interesting example of evidence related to machine-produced documents that was considered not to be relevant appears in the High Court case of *Smith v The Queen* [2001] HCA 50 (16 August 2001). At trial, the prosecution had tendered bank security camera photos purportedly identifying the accused as present at the scene of a robbery, and had called police officers familiar with the accused to identify him as the person in the photos. The High Court held that this evidence had been wrongly admitted, as it could not rationally affect the jury's assessment of whether the photo matched the physical appearance of the accused, who was present in court.

Evidence which is otherwise relevant may be excluded as hearsay, which means it is evidence of a previous representation (typically in communications at or following the events which are the subject of the proceeding) and which is tendered to try to prove the truth of the representation. Such evidence is excluded unless an exception applies (s59). Various exceptions are set out in the Evidence Act, which may apply also to electronic evidence, but three exceptions are worth particular mention.

Section 69 provides a general exception to the hearsay rule in s59 in relation to business records. These are defined as documents that form 'part of the records belonging to or kept by a person, body or organisation in the course of, or for the purposes of, a business', and the term business is further broadly defined (Part 2 of the Dictionary) as 'a profession, calling, occupation, trade or undertaking', or Parliamentary or governmental business, whether conducted for profit or not, or carried out in or outside Australia. Documents such as cash register rolls, transactional statements and customer lists will usually be accepted as business records, but it should be noted that not every document associated with a business will necessarily constitute a business record – for example, in the case of *Roach & Ors v Page & Ors* (No.27) [2003] NSWSC 1046 (13 November 2003) the contents of corporate websites were not admitted under s69. Another example appears in the New South Wales case of *Roads and Traffic Authority of New South Wales v Tetley* [2004] NSWSC 925 (8 October 2004). Duplicates of driver logbooks and journey report (computer-generated print-out derived from a Global Positioning System/vehicle monitoring information system) were ruled inadmissible under s69 of the Evidence Act.

The books of accounts provisions in subsections 83–91 of the *Evidence Act 1977* (Qld) may provide a general exception in relation to business records (QLRC 2005). Where the business records are held electronically, Section 95 of the *Evidence Act 1977* (Qld) may also apply if business records are held electronically.

Section 70 provides an exception to the hearsay rule (s59) for tags, labels and similar writing that is or has been placed on an object (including a document) during the course of business 'for the purpose of describing or stating the identity, nature, ownership, destination, origin or weight of the object, or of the contents (if any) of the object'. This may in some circumstances apply to electronic evidence, for example, in relation to the file directory and similar details that added automatically in the footer space of some documents.

Section 71 provides an exception to the hearsay rule (s59) for representations in documents 'recording a message that has been transmitted by electronic mail or by a fax, telegram, lettergram or telex' that relate to identity of sender or recipient, destination or time. This exception is supplemented by Division 3 of Part 4.3 of the Act, which deals with such forms of communication.

In addition to the hearsay exclusionary rules, there is a range of other exclusions that may relate to electronic evidence. These include the *opinion* rule (s69), rules about evidence of *judgments* and *convictions* (s91), the *tendency* (s97) and *coincidence* (s98) rules, the *credibility* (s102) and *character* (s110) rules, and *identification rules* (ss114 and ss115). For all of these rules, there are exceptions that may operate. To give just one example, electronic evidence of a defendant's internet browsing habits may be adduced to try to prove that the defendant had a particular interest in a type of material (such as child pornography). This evidence (if considered relevant) might be excluded as tendency evidence (s97) unless it is of significant probative value, but even if it meets this test, must still be excluded (s101) as prosecution evidence unless 'the probative value of the evidence substantially outweighs any prejudicial effect it may have on the defendant' (see *R v MM* [2004] NSWCCA 364).

Evidence which is otherwise admissible may still be excluded if its probative value is substantially outweighed by the danger that the evidence might be unfairly prejudicial, be misleading or confusing, or cause or result in undue waste of time (s135). In criminal proceedings, prosecution evidence must be excluded if its probative value is outweighed by the danger of unfair prejudice to the defendant (s137). Unfair prejudice may arise where there is a danger that evidence will be misused or misunderstood by a jury, or where a party is unable to cross-examine the maker of a statement that has been admitted into evidence (see *Roach & Ors v Page and Ors* (No. 11) [2003] NSWSC 907). The use of evidence may also be limited by the court (s136).

Discretionary exclusion also applies in the case of improperly or illegally obtained evidence (s138), which is most likely to be raised in the context of electronic evidence where a valid search warrant has not been obtained prior to forensic examination of a computer, or the search goes beyond what is authorised by the warrant (*ASIC v Rich* [2005] NSWSC 62 (16 February 2005); *R v PJ* [2006] ACTS 37 (2 May 2006), discussed above).

Opinions based on specialised knowledge

Under s79 (an exception to the exclusionary opinion rule in s76) of the *Evidence Act 1995* (Cth), a court may admit opinion evidence from a witness who has specialised knowledge:

> If a person has specialised knowledge based on the person's training, study or experience, the opinion rule does not apply to evidence of an opinion of that person that is wholly or substantially based on that knowledge.

The requirements that the witness's specialised knowledge be 'based on the person's training, study or experience' and that the opinion in turn be 'wholly or substantially based on that knowledge' are important limitations in the circumstances in which specialist opinion evidence may be admitted. Unlike the United States, Australian law does not require proof of expertise in a recognised field of scientific knowledge (as per the test in *Daubert v Merrell Dow Pharmaceuticals* 509 US 579 (1993)), but rather allows a person's training, study or (non-academic) work experience to ground a specialist opinion. The Daubert test, a widely accepted legal test to determine the validity of scientific evidence and its relevance to the case at issue, examines the following criteria:

- Tested – Has the scientific theory or technique been tested?
- Peer reviewed – Has the scientific theory or technique been subjected to peer review (by other experts in the field) and publication?
- Error rate – What is the known or potential error rate (i.e. type I and type II error)?
- Standards and Acceptance – What is the expert's qualifications and stature in the scientific community? And does the technique rely upon the special skills and equipment of one expert, or can it be replicated by other experts elsewhere?

However, it has been held that opinion based on specialist expertise does not necessarily fall within the terms of s79 if it involves an extension of existing expertise to a new field of inquiry not substantially linked to the person's specialist training: see *R v Hien Puoc Tang* [2006] NSWCCA 167 (24 May 2006), a case concerning computer-assisted facial and body mapping.

The following statement is widely accepted as definitively setting out the requirements of s79 of the *Evidence Act*, per Heydon JA in *Makita (Australia) Pty Ltd v Sprowles* [2001] NSWCA 305 (14 September 2001):

> In short, if evidence tendered as expert opinion evidence is to be admissible, it must be agreed or demonstrated that there is a field of 'specialised knowledge'; there must be an identified aspect of that field in which the witness demonstrates that by reason of specified training, study or experience, the witness has become an expert; the opinion proffered must be 'wholly or substantially based on the witness's expert knowledge'; so far as the opinion is based on facts 'observed' by the expert, they must be identified and admissibly proved by the expert, and so far as the opinion is based on 'assumed' or 'accepted' facts, they must be identified and proved in some other way; it must be established that the facts on which the opinion is based form a proper foundation for it; and the opinion of an expert requires demonstration or examination of the scientific or other intellectual basis of the conclusions reached: that is, the expert's evidence must explain how the field of 'specialised knowledge' in which the witness is expert by reason of 'training, study or experience', and on which the opinion is 'wholly or substantially based', applies to the facts assumed or observed so as to produce the opinion propounded. If all these matters are not made explicit, it is not possible to be sure whether the opinion is based wholly or substantially on the expert's specialised knowledge. If the court cannot be sure of that, the evidence is strictly speaking not admissible, and, so far as it is admissible, of diminished weight.

In the context of computer forensics, there is no particular level of training, study or experience that must be established for a person to be able to give evidence in proceedings. The witness's qualifications will usually be a matter for the court to assess on a voir dire (s189 of the uniform Evidence Act), and the usual matters taken into account include degrees or diplomas held, specialist courses undertaken, workplace training, and practical experience (in Victoria see s391A of the *Crimes Act 1958*), Experts are also required to comply with the procedures of the court, such as providing a certificate of expert evidence required under Section 177 of the *Evidence Act 1995* (Cth).

In contested criminal proceedings involving computer-related offences, the prosecution will often call its own expert witnesses, and the defence may call opposing experts to try to cast doubt on parts of the prosecution case. Where both prosecution and defence experts have given evidence on technical matters, the weight to be given to the opinions presented is a matter for the jury or other fact-finder (*R v Lisoff* [1999] NSWCCA 364 (22 November 1999)).

Juror comprehension and the use of courtroom technologies

Particular challenges can arise in technology-enabled crime cases where juries are involved. Juries will usually be present in contested trials for more serious criminal offences (i.e. indictable rather than summary offences) and less commonly in civil litigation. Geisler (2004: 32) explains the challenge for the security expert in communicating technical information to jurors thus:

> The expert witness must be able to outline, as clearly and succinctly as possible, how his/her conclusions were reached and the underlying methodology for those conclusions. The security expert must educate the jury by providing it with the information needed to ultimately decide the disputed facts, together with a framework in which to process the information. It is not enough to merely state conclusions backed up with only the expert's credentials and expertise.
>
> Security experts must be able to clearly articulate 'why' and 'how' their conclusions were reached, in a way that is clear, simple and direct. However, this process involves more than an organized analytical framework; it requires the expert to first understand the jury's expectations and to deliver the information accordingly.

Similar concerns have been raised by researchers. For example Sprague (2006) suggested that:

> [c]omputer crime prosecutions very often are, or can be forced into being, a form of 'complex litigation,' chock full of confusing technological terms and concepts. The average juror is generally ignorant of both the theory and practice of computer science. Even 'computer savvy' jurors are unlikely to have the training or experience to comprehend complex issues involving networking, security theory and practice, computer architecture, operating systems, system administration, or programming. A conscientious juror may well (and should) have a problem concluding that all reasonable doubt has been eliminated by evidence that he or she does not fully understand (Sprague 2006: 145).

The judge in the Federal Court of Australia case of *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2002] FCA 906 (26 July 2002) also indicated that '[t]he Court should not be left in a position where it has to guess as to the operation of technological processes and how those processes might satisfy the statutory language'. Such (technical) information that needs to be communicated to the judiciary by the security experts includes:

- the possibility for a wide variety of evidence to be extracted from an increasing diversity in sources of computer or electronic exhibits (e.g. GPS devices, engine management systems, CCTV systems, digital cameras and mobile phones)
- the use of mathematical hash algorithms in computer forensics as a means of evidence authentication to be able to trust the hash values that uniquely identify electronic evidence
- the use of filtering to reduce data volumes including the use of hash sets or targeted searching as their use or non-use may have significant impact on processing time, and accuracy of the results
- visualising the actual size of digital data as it has been noted that in a number of court case trials, judges, prosecutors and unassisted defence lawyers have asked for all data on a computer exhibit to be printed out. In many technology-enabled cases, a printout of all data produced as a result of an examination will be infeasible. For example, the amount of information gathered during the investigation in Operation Firewall by the United States Secret Services is estimated to be approximately two terabytes – the equivalent of an average university's academic library (USSS 2004). Moreover, hardcopy printout of an electronic document does not necessarily include all the information stored in the computer or electronic exhibit (e.g. data held in memory) (see *Armstrong v Executive Office of the President* 1 F 3d 1274 (DC Cir 1993)).

Lederer (2004) suggested that '[h]igh-tech trials are predominantly visual trials. For that to be true, images must be able to be seen. Most high-tech courtrooms provide the judge, witness, and counsel with small flat screen (LCD) monitors'. State-of-the-art courtroom technologies (e.g. visual communication technologies including videoconferencing, presentation software, computer animations and simulations and digital video) in technology-enabled crime prosecutions can, therefore, be an efficient tool in judiciary comprehension of electronic evidence (Lederer 2002). For example, document cameras allow users to place documents or objects on the presenter, take a photo of the document or objects and transmit the image to a screen. The ability to highlight and zoom-in on critical parts of the document will be helpful in simplifying complex concepts to the judiciary. It was also noted that

> … the new visual technologies and current trends in the mass mediazation of culture offer advocates especially powerful ways to evoke fictional models for events and behavior and to increase the likelihood that jurors and judges will use those models (uncritically) in reaching their decisions (Feigenson & Dunn 2003: 122).

In Australia, courtroom technologies are being built into or retrofitted into courtrooms as appropriate. A summary of available courtroom technology in Australia's higher courts is described in Table 7.

Table 7: Summary of available courtroom technology in Australia's supreme courts

Supreme Court	Document camera	Projector and screen	Digital audio facilities	Computers/ laptops	Internet	Plasma/ LCD monitors	Individual monitors for jury and/or witness
Cth	√	√	√		√	√	√
ACT		√					√
NSW	√	√	√	√	√	√	√
NT			√			√	
Qld	√	√	√	√	√	√	√
SA	√	√	√			√	√
Tas	√	√	√	Available to judges only		√	
Vic	√	√	√		√	√	
WA	√	√	√			√	√

a. Personal communication, Dorothy Shea (Librarian of the Supreme Court of Tasmania) to Australian Institute of Criminology (2 May 2007)

Source: Adapted from De Wilde (2006: 325-326). Information was correct as at January 2006.

Legal and other privileges

Another basis on which the admission of electronic evidence may be challenged is with a claim of legal or other type of privilege. The main types of privilege dealt with under the uniform Evidence Acts are:

- client legal privilege (known in common law and some other legislation as legal professional privilege), found in Division 1 of Part 3.10 of all three Acts (also in s19D of the *Evidence Act 1958* (Vic))
- professional confidential relationships privilege, found in Division 1A of the NSW Act only
- sexual assault communications privilege, found in Division 1B of the NSW Act only
- medical communications privilege, found in s127A of the Tas Act only (also in s12(2) of the *Evidence Act* (NT) and ss28(2)–(5) of the *Evidence Act 1958* (Vic))
- communications with a counsellor by a victim of a sexual offence privilege, found in s127B of the Tas Act only (also in s67F of the *Evidence Act 1929* (SA), ss56–56G of the *Evidence Act* (NT) and Division 2A of Part II *Evidence Act 1958* (Vic))
- privilege against self-incrimination, found in s128 of all three Acts.

Although the privilege against self-incrimination is also dealt with under s10 *Evidence Act 1977* (Qld), it is abrogated, in part, by ss15(1), which provides that an accused in a criminal proceeding shall not be entitled to refuse to answer a question or produce a document or thing on the ground that to do so would tend to prove the commission by the person of the offence with which the person is there charged.

In addition, there is range of other privileges in Divisions 3 of Part 3.10 of the uniform Evidence Acts, which deals with evidence excluded in the public interest. This includes:

- evidence of reasons for judicial and similar decisions (s129)
- evidence of matters of state (s130)
- evidence of settlement negotiations (s131).

It should also be noted that other legislation may restrict the ability of parties to adduce, or to be given access to, security sensitive or otherwise restricted information in some proceedings. For example, the

National Security Information (Criminal Proceedings) Act 2004 (Cth) provides mechanisms whereby such information may be used in criminal proceedings without risk of public disclosure.

The court must also be satisfied that witnesses are aware of their rights in relation to privileges as provided by s132 of the uniform Evidence Acts.

Client legal privilege

Under the uniform Evidence Acts, evidence is not to be admitted if, on objection from a client, the court finds that adducing the evidence would result in the disclosure of confidential communication made between lawyer and client or a confidential document prepared for the dominant purpose of advising the client (s118) or preparing for litigation (s119). It should be noted that advice privilege does not extend to third party communications under s118. For example, in the New South Wales case of *Westpac Banking Corporation v 789TEN Pty Ltd* [2005] NSWCA 321 (19 September 2005), an appeal against the judgment by the trial judge, Mr Justice Bergin, that the letters were not privileged under s118 as the 'provision relevantly protected documents prepared for the dominant purpose of a lawyer providing legal advice to a client' was dismissed.

Claims of client legal privilege may particularly arise where lawyers' offices or computers, or those of other professionals, are being searched for evidence. Because electronic communications technologies such as fax, email and instant messaging are increasingly used for business and other dealings, it is to be expected that claims of client legal privilege will increasingly focus on such communications: see, for example, *In the matter of Bauhaus Pyrmont Pty Ltd (in liq)* [2006] NSWSC 543 (6 June 2006).

Despite the prevalence of computers and other electronic devices in communications, there is some uncertainty about how potential claims of client legal privilege are to be dealt with in the execution of search warrants covering computer contents. The AFP and the Law Council of Australia (LCA) in 1990 agreed a set of guidelines on AFP searches where claims of legal professional privilege arise, which were revised in 1997, but these do not make any reference to computer records (LCA 1990).

At present the procedures to be followed relate only to physical documents rather than computer contents or records of electronic communications (par 24–25):

> Where the lawyer or Law Society agrees to assist the search team the procedures set out below should be followed:-
>
> (a) in respect of all documents identified by the lawyer or Law Society and/or further identified by the executing officer as potentially within the warrant, the executing officer should, before proceeding to further execute the warrant (by inspection or otherwise) and to seize the documents, give the lawyer or Law Society the opportunity to claim legal professional privilege in respect of any of those documents
>
> (b) if the lawyer or Law Society asserts a claim of legal professional privilege in relation to any of those documents then the lawyer or Law Society should be prepared to indicate to the executing officer the grounds upon which the claim is made and in whose name the claim is made
>
> (c) in respect of those documents which the lawyer or Law Society claim are subject to legal professional privilege, the search team shall proceed in accordance with the guidelines as follows. In respect of the remaining documents, the search team may then proceed to complete the execution of warrant.
>
> ….
>
> All documents which the lawyer or Law Society claims are subject to legal professional privilege shall under the supervision of the executing officer be placed by the lawyer and/or his/her staff, or the Law Society and/or its representatives, in a container which shall then be sealed.

Similar LCA guidelines have been agreed in relation to Australian Taxation Office (ATO) access to lawyers' premises (LCA 1991). However, these remain unamended since being issued in 1991. As with the AFP Guidelines, such policies should be updated to reflect their application to computer contents and electronic communications, and in particular to refer to the search warrant provisions under Commonwealth law introduced into the *Crimes Act 1914* (Cth) and *Customs Act 1901* (Cth) by the *Cybercrime Act 2001* (Cth).

Bibliography

URLs were correct at 7 Febuary 2008

Australian Institute of Criminology publications

Crime facts info

no. 134. The costs of high tech crime. http://www.aic.gov.au/publications/cfi/cfi134.html

High tech crime briefs

no. 1. *Concepts and terms*. http://www.aic.gov.au/publications/htcb/htcb001.html

no. 2. *Child exploitation*. http://www.aic.gov.au/publications/htcb/htcb002.html

no. 3. *Copyright offences*. http://www.aic.gov.au/publications/htcb/htcb003.html

no. 4. *Evidence*. http://www.aic.gov.au/publications/htcb/htcb004.html

no. 5. *Hacking offences*. http://www.aic.gov.au/publications/htcb/htcb005.html

no. 6. *Hacking motives*. http://www.aic.gov.au/publications/htcb/htcb006.html

no. 7. *Hacking techniques*. http://www.aic.gov.au/publications/htcb/htcb007.html

no. 8. *Child pornography sentencing in NSW*. http://www.aic.gov.au/publications/htcb/htcb008.html

no. 9. *Phishing*. http://www.aic.gov.au/publications/htcb/htcb009.html

no. 10. *Malware: viruses, worms, Trojan horses*. http://www.aic.gov.au/publications/htcb/htcb010.html

no. 11. *More malware: adware, spyware, spam and spim*. http://www.aic.gov.au/publications/htcb/htcb011.html

no. 12. *High tech crime tools*. http://www.aic.gov.au/publications/htcb/htcb012.html

no. 13. *Acquiring high tech crime tools*. http://www.aic.gov.au/publications/htcb/htcb013.html

no. 14. *New methods of transferring value electronically*. http://www.aic.gov.au/publications/htcb/htcb014.html

no. 15. *The risk of criminal exploitation of online auctions*. http://www.aic.gov.au/publications/htcb/htcb015.html

no. 16. *Money mules*. http://www.aic.gov.au/publications/htcb/htcb016.html

Trends & issues in crime and criminal justice

no. 97. Forde P & Patterson A 1998. Paedophile internet activity. http://www.aic.gov.au/publications/tandi/tandi97.html

no. 118. McKemmish R 1999. What is forensic computing? http://www.aic.gov.au/publications/tandi/tandi118.html

no. 294. McCusker R 2005. Spam: nuisance or menace, prevention or cure? http://www.aic.gov.au/publications/tandi2/tandi294.html

no. 299. Krone T 2005a. Does thinking make it so? Defining online child pornography possession offences. http://www.aic.gov.au/publications/tandi2/tandi299.html

no. 301. Krone T 2005b. Queensland police stings in online chat rooms. http://www.aic.gov.au/publications/tandi2/tandi301.html

no. 329. Urbas G & Krone T 2006. Mobile and wireless technologies: security and risk factors. http://www.aic.gov.au/publications/tandi2/tandi329.html

no. 330. Krone T & Johnson H 2006. Internet purchasing : perceptions and experiences of Australian households. http://www.aic.gov.au/publications/tandi2/tandi330.html

Research and public policy series

no. 39. Smith R & Urbas G 2001. *Controlling fraud on the internet: A CAPa perspective: report for the Confederation of Asian and Pacific Accountants*. http://www.aic.gov.au/publications/rpp/39/index.html

no. 60. Charlton K & Taylor N 2004. *Online credit card fraud against small businesses*. http://www.aic.gov.au/publications/rpp/60/index.html

no. 64. Johnson H 2005. *Crime victimisation in Australia: key results of the 2004 International Crime Victimisation Survey*. http://www.aic.gov.au/publications/rpp/64/index.html

no. 78. Choo KKR, Smith RG & McCusker R 2007. *Future directions in technology-enabled crime 2007–09*. http://www.aic.gov.au/publications/rpp/78/index.html

Other publications

AusCERT 2006. *Computer crime and security survey.* http://www.auscert.org.au/render.html?it=2001

Australia. Attorney-General's Department (AGD) 2005. A new extradition system: a review of Australia's extradition law and practice. Canberra: AGD. http://www.ag.gov.au/www/agd/agd.nsf/Page/Extraditionandmutualassistance_Extraditiondiscussionpaper

Australia. Department of Communications, Information Technology and the Arts (DCITA) 2006. *Spam report*. Canberra: DCITA. http://www.dcita.gov.au/communications_and_technology/publications_and_reports/2003/04/spam_report

Australian Communications and Media Authority (ACMA) 2005. Racing tips company fined for breach of Spam Act. *Media release* 17 August. http://www.acma.gov.au/WEB/STANDARD//pc=PC_100121

Australian Communications and Media Authority (ACMA) 2007. Internet complaints February 2007. *ACMAsphere* Issue 18, April: 19

Australian Customs Service 2007a. UK visitor charged with child pornography offence. *Media release* 2 August. http://www.customs.gov.au/site/page.cfm?c=9200

Australian Customs Service 2007b. $9000 fine for importing child pornography. *Media release* 14 August. http://www.customs.gov.au/site/page.cfm?c=9256

Australian Federal Police (AFP) 2007. Two men in two states charged over child pornography. *Media release* 3 August. http://www.afp.gov.au/media_releases/national/2007/two_men_in_two_states_charged_over.html

Australian High Tech Crime Centre (AHTCC) 2006. International internet investigation nets arrest. *Media release* 22 March

Australian Law Reform Commission (ALRC) 2005. *Review of the Uniform Evidence Acts*. Discussion Paper 69. Sydney: ALRC. http://www.austlii.edu.au/au/other/alrc/publications/dp/69/

Beyer A 2004. Defamation on the internet: Joseph Gutnick v Dow Jones. *E-law: Murdoch University electronic journal of law* 11(3). http://www.murdoch.edu.au/elaw/issues/v11n3/beyer113.html

Black MEJ 2007. *Practice direction: guidelines for expert witnesses in proceedings in the Federal Court of Australia*. Sydney: Federal Court of Australia. http://www.fedcourt.gov.au/how/prac_direction.html#current

Blackwood J & Warner K 1993. *Tasmanian criminal law: text and cases*. Hobart: University of Tasmania

Brenner SW 2001. Cybercrime investigation and prosecution: the role of penal and procedural law. *E-law: Murdoch University electronic journal of law* 8(2). http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html

Brenner SW, Carrier B & Henninger J 2004. The Trojan horse defense in cybercrime cases. *Santa Clara computer and high tech law journal* 21: 1. http://www.chtlj.org/pdf/21-1_Brenner.pdf [.1]

Broersma M 2007. Spam shows sudden slide. *Computerworld.com* 10 January

Bronitt S & Gani M 2003. Shifting boundaries of cybercrime: from computer hacking to cyberterrorism. *Criminal law journal* 27: 303-321

Bronitt S & McSherry B 2005. *Principles of criminal law*, 2nd ed. Sydney: Thomson Lawbook Co.

Casey E 2002. Error, uncertainty, and loss in digital evidence. *International journal of digital evidence* 1(2). http://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf

Commonwealth Director of Public Prosecutions 2006. *2005–2006 annual report*. Canberra: CDPP. http://www.cdpp.gov.au/AboutUs/AnnualReports/

Cuthbertson S 2001. Mutual assistance in criminal matters: beyond 2000. *Australian law journal* 75(5): 326–336

De Wilde F 2006. Courtroom technology in Australian courts: an exploration into its availability, use and acceptance. *Qld lawyer* 26: 303–328

Dreyfus S 1997. Judgement Day. *Underground: tales of hacking, madness and obsession on the electronic frontier*: chapter 7. http://jmason.org/underground/chapter_7.html

Federal Bureau of Investigation (FBI) 2003a. The case of the hacked South Pole. *Media release* 18 July. http://www.fbi.gov/page2/july03/071803backsp.htm

Feigenson N & Dunn MA 2003. New visual technologies in court: directions for research. *Law and human behavior* 27(1): 109–126

Fox R & Freiberg A 1999. *Sentencing: state and federal law in Victoria*, 2nd ed. South Melbourne: Oxford University Press

Geisler LB 2004. Expert issues arising during trial: effectively communicating complex concepts to jurors. *Security journal* 17(3): 31–39

Goodin D 2007. Man faces 10 years for fudging computer credentials. *The Register* 9 May. http://www.theregister.co.uk/2007/05/09/computer_expert_pleads_guilty/

Goodman MD & Brenner SW 2002. The emerging consensus on criminal conduct in cyberspace. *UCLA journal of law and technology* 3. http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php

Grant A, David F & Grabosky PN 1997. Child pornography in the digital age. *Transnational organized crime* 3(4): 171–188. http://www.aic.gov.au/publications/chpornography/

Grabosky PN & Smith RG 1998. *Crime in the digital age: controlling telecommunications and cyberspace illegalities*. New Brunswick, NJ: Transaction Publishers

Grabosky PN, Smith RG & Dempsey G 2001. *Electronic Theft: unlawful acquisition in cyberspace*. Cambridge University Press

Harding T 2007. Terrorists use Google maps to hit UK troops. *Telegraph.co.uk* 13 January. http://www. telegraph.co.uk/news/main.jhtml?xml=/news/2007/01/13/wgoogle13.xml

Hayes S 2006. Local fights US piracy charges. *AustralianIT* 10 January.

Hutchinson W & Warren M 2001 *Information warfare: corporate attack and defence in a digital world*. Oxford: Butterworth-Heinemann

James NJ 2004. Handing over the keys: contingency, power and resistance in the context of section 3LA of the Australian Crimes Act 1914. *University of Queensland law journal* 23(1): 7-21

Jen WY, Chang W & Chou S 2006. Cybercrime in Taiwan: an analysis of suspect records. *Lecture notes in computer science* 3917: 38–48

Kshetri N 2006. The simple economics of cybercrimes. *IEEE security & privacy* 4(1): 33–39

Krone T 2006. Gaps in cyberspace can leave us vulnerable. *Platypus magazine* 90: 31-37

Law Council of Australia (LCA) 1990. Execution of AFP search warrants on lawyers' premises. http://www.lawcouncil.asn.au/policy/1959496083.html

Law Council of Australia (LCA) 1991. Australian Taxation Office access to lawyers' premises. http://www.lawcouncil.asn.au/policy/1959496147.html

Lebihan R 2006. Judge makes mincemeat of spammer with $5m fine. *Australian financial review* 28 October

Lederer Fl 2002. The road to the virtual courtroom? A consideration of today's and tomorrow's high tech courtrooms. Paper to the International conference on technology and its effects on criminal responsibility, security and criminal justice, 9 December, Charleston, South Carolina

Lederer Fl 2004. Courtroom technology: for trial lawyers, the future is now. *Criminal justice magazine* 19(1). http://www.abanet.org/crimjust/cjmag/19-1/courtroomtech.html

Maury S 2004. Developments in combating cyberstalking in Australia. *Internet Law Bulletin* 6(10): 126–128

McAfee 2005. *McAfee virtual criminology report*. Santa Clara CA: McAfee.

Mitchell KJ, Wolak J & Finkelhor D 2005. Police posing as juveniles online to catch sex offenders: is it working? *Sexual abuse* 17(3): 241–267

Model Criminal Law Officers' Committee (MCLOC) of the Standing Committee of Attorneys-General Australia 2007. *Identity crime: discussion paper*. Barton AGD. http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4341200FE1255EFC59DB7A1770C1D0A5)~MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf/$file/MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf

Model Criminal Code Officers Committee (MCCOC) of the Standing Committee of Attorneys-General Australia 2001. *Damage and computer offences*. Barton AGD

National Institute of Standards and Technology (NIST) 2006a. *Guide to integrating forensic techniques into incident response*. NIST computer security special publications SP800-86. Rockville MD: NIST. http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

National Institute of Standards and Technology (NIST) 2006b. *Guide to computer security log management*. NIST computer security special publications SP800-92. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

New South Wales Law Reform Commission (NSW LRC) 2004. *Expert witnesses*. Issues paper 25. Sydney: NSWLRC. http://www.lawlink.nsw.gov.au/lrc.nsf/pages/ip25toc

New South Wales Police (NSW Police) 2007. Man charged with child grooming offences - child exploitation internet unit. *Media release* 28 March

Organisation for Economic Development (OECD) 2002. *Guidelines for the security of information systems and networks: towards a culture of security*. Paris: OECD. http://www.oecd.org/dataoecd/16/22/15582260.pdf

Organisation for Economic Development (OECD) 2005. *The promotion of a culture of security for information systems and networks in OECD countries*. Paris: OECD. http://www.oecd.org/dataoecd/16/27/35884541.pdf

Queensland Law Reform Commission (QLRC) 2005. A review of the uniform evidence Acts. Report no. 60. Brisbane: QLRC. http://www.qlrc.qld.gov.au/reports/r60.pdf

PricewaterhouseCoopers (PWC) 2006. *DTI information security breaches survey 2006*. London: Department of Trade and Industry. http://www.pwc.com/extweb/pwcpublications.nsf/docid/7FA80D2B30A116D7802570B9005C3D16

Republic of China 2006. *Second G8 training conference for 24/7 points of contact*. Official publications echo network. (Document in mandarin). http://open.nat.gov.tw/OpenFront/report/show_file.jsp?sysId=C09600684&fileNo=001

Sieber U 1998. *Legal aspects of computer-related crime in the information society*. Comcrime Study executive summary. Brussels: European Commission. http://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html

Smith R, Grabosky P & Urbas G 2004. *Cyber criminals on trial*. Port Melbourne: Cambridge University Press

Speer DL 2000. Redefining borders: The challenges of cybercrime. *Crime, law and social change* 34: 259–273

Sprague WE 2006. Uncharted waters: prosecuting phishing and online fraud cases. *Journal of digital forensic practice* 1: 143–146

Steel A 2002. Vaguely going where no-one has gone: the expansive new computer access offences. *Criminal law journal* 26: 72–97

Sydney Morning Herald (SMH) 2006. Man jailed in landmark internet sex case. *SMH.com.au* 21 June. http://www.smh.com.au/news/technology/man-jailed-in-landmark-internet-sex-case/2006/07/21/1153166569887.html

Sydney Morning Herald (SMH) 2007. Selim cleared over destruction of data. *SMH.com.au* 19 April. http://www.smh.com.au/news/national/selim-cleared-over-destruction-of-data/2007/04/18/1176696916796.html#

Symantec 2005. *Symantec spam statistics*. Cupertino CA: Symantec. http://www.symantec.com/region/reg_ap/promo/brightmail/docs/May2005SpamStats.pdf

Tasmania. House of Assembly 2005 (various speakers). Criminal Code Amendment (Child Exploitation) Bill 2005 (No. 37): Second reading. Hansard 14 June. http://www.hansard.parliament.tas.gov.au/isysquery/irle10d/1/doc

Thompson DE & Berwick DR 1998. *Minimum provisions for the investigation of computer based offences*. Report series no. 129.1. Payneham: National Police Research Unit

United Nations 2000. Challenge of borderless ‘cyber-crime’ to international efforts to combat transnational organized crime discussed at Symposium. *Media release* 14 December. http://www.unis.unvienna.org/unis/pressrels/2000/LPMO10.html

United Nations Commission on Crime Prevention and Criminal Justice 2001. *Revised draft plans of action for the implementation of the Vienna Declaration on Crime and Justice: meeting the challenges of the twenty-first century*. http://www.undcp.org/pdf/crime/10_commission/resumed_session/14e.pdf

United Nations 2005. Eleventh UN crime congress opens in Bangkok with focus on organized crime, terrorism. *Media release* SOC/CP/322. 19 April. http://www.un.org/News/Press/docs/2005/soccp322.doc.htm

United States Air Force (USAF) 2005. Global Network Operations co-host annual conference. *Media release # 2005-02*. 8 December. http://www.dc3.mil/dcci/confprrelease.doc

United States. Department of Justice (US DoJ) 2003b. Defendant indicted in connection with operating illegal internet software piracy group. *Media release* 12 March. http://www.cybercrime.gov/griffithsIndict.htm

United States. Department of Justice (US DoJ) 2005. Justice department announces international internet piracy sweep. *Media release* 30 June. http://www.usdoj.gov/criminal/cybercrime/OperationSiteDown.htm

United States Department of Justice (US DoJ) 2006. Prepared remarks of attorney general Alberto r. Gonzales at announcement of criminal charges in international, internet-based child pornography investigation. *Media release* 15 March. http://www.usdoj.gov/ag/speeches/2006/ag_speech_060315.html

United States. Department of Justice (US DoJ) 2007a. Bogus expert in computer forensics pleads guilty to perjury charges. *Media release* 4 May. http://www.usdoj.gov/usao/cae/press_releases/docs/2007/05-04-07EdmistonPlea.pdf

United States. Department of Justice (US DoJ) 2007b. Electronic funds transfer fraud. *Media release* 8 May. http://cleveland.fbi.gov/dojpressrel/2007/fraud050807.htm

United States. Department of Justice (US DoJ) 2007c. Extradited software piracy ringleader pleads guilty. *Media release* 20 April. http://washingtondc.fbi.gov/dojpressrel/pressrel07/wfo042007b.htm

United States. Department of Justice (US DoJ) 2007d. Extradited software piracy ringleader sentenced to 51 months in prison. *Media release* 22 June. http://washingtondc.fbi.gov/dojpressrel/pressrel07/wfo062207.htm

United States. Department of Justice (US DoJ) 2007e. Former member of the US navy indicted on terrorism and espionage charges. *Media release* 31 March. http://newhaven.fbi.gov/dojpressrel/2007/nh032107.htm

United States. Department of Justice (US DoJ) 2007f. Software piracy ringleader extradited from Australia. *Media release* 20 February. http://www.usdoj.gov/criminal/cybercrime/griffithsExtradition.htm

United States. Department of Justice (US DoJ) 2007g. U.S. arrests Manhattan consultant for travelling between states to engage in sexual activities with a minor under the age of 12. *Media release* 17 July

United States. Federal Bureau of Investigation (US FBI) 2007. Santa Clarita man indicted today for using internet to entice minor into sex. *Media release* 3 January http://losangeles.fbi.gov/pressrel/2007/la010307.htm

United States Secret Service (USSS) 2004. U.S. secret service's operation firewall nets 28 arrests. *Media release* 28 October

Urbas G 2005. Cyber-terrorism and Australian law. *Internet law bulletin* 8(1): 5–7

Young K 1996. Internet addiction: the emergence of a new clinical disorder. *Cyber psychology and behavior* 3: 237–244

Cases

DPP v Sutcliffe [2001] VSC 43 (1 March 2001)

Williams v Keelty [2001] FCA 1301 (13 September 2001)

R v Boden [2002] QCA 164 (10 May 2002)

Hart v Commissioner, AFP [2002] FCAFC 392 (5 December 2002)

Jones v Toben [2002] FCA 1150 (17 September 2002)

Dow Jones v Gutnick [2002] HCA 56 (10 December 2002)

R v Magoulias [2003] NSWCCA 143 (26 May 2003)

Grant v Marshall [2003] FCA 1611 (19 September 2003)

Roach & Ors v Page and Ors (No. 11) [2003] NSWSC 907 (10 October 2003)

Kennedy v Baker [2004] FCA 562 (6 May 2004)

R v Kennings [2004] QCA 162 (14 May 2004)

ASIC v Rich [2005] NSWSC 62 (16 February 2005)

Griffiths v United States of America [2005] FCAFC 34 (10 March 2005)

R v Shetty [2005] QCA 225 (24 June 2005)

Oke v Commissioner of the Australian Federal Police [2005] FCA 1363 (20 September 2005)

R v PJ [2006] ACTSC 37 (2 May 2006)

Egglishaw v Australian Crime Commission [2006] FCA 819 (30 June 2006)

DPP (NSW) v KEAR, Martin [2006] NSWSC 1145

Universal Music Australia Pty Ltd v Cooper [2005] FCA 972 (14 July 2005)

Regina v Lodhi [2006] NSWSC 691 (23 August 2006)

R V Ferguson [2006] 3 DCLR(NSW) 70 (9 March 2006)

Roads and Traffic Authority of New South Wales v Tetley [2004] NSWSC 925 (8 October 2004)

Kabushiki Kaisha Sony Computer Entertainment v Stevens [2002] FCA 906 (26 July 2002)

Westpac Banking Corporation v 789TEN Pty Ltd [2005] NSWCA 321 (19 September 2005)

Peach v Bird 159 A Crim R 416 [2006] NTSC 14 (21 February 2006)

Legislation

Criminal Code Act 1995 (Cth)

Crimes Act 1914 (Cth)

Cybercime Act 2001 (Cth)

Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004 (Cth)

Privacy Act 1988 (Cth)

Telecommunications Act 1997 (Cth)

Crimes Act 1900 (ACT)

Criminal Code 2002 (ACT)

Crimes Act 1900 (NSW)

Crimes Amendment (Computer Offences) Act 2001 (NSW)

Criminal Code (NT)

Criminal Code Amendment Act 2001 (NT)

Criminal Code Act 1899 (Qld)

Criminal Law Amendment Act 1997 (Qld)

Criminal Law Consolidation Act 1935 (SA)

Summary Offences Act 1953 (SA)

Summary Offences Act Amendment Act 1989 (SA)

Summary Offences (Offensive and Other Weapons) Amendment Act 1998 (SA)

Statutes Amendment (Computer Offences) Act 2004 (SA)

Criminal Code Act 1924 (Tas)

Criminal Law Amendment Act 1990 (Tas)

Crimes Act 1958 (Vic)

Crimes (Property Damage and Computer Offences) Act 2003 (Vic)

Criminal Code (WA)

Criminal Law Amendment (Simple Offences) Act 2004 (WA)

International instruments

Council of Europe, *Convention on Cybercrime*: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Council of Europe, Additional Protocol to the *Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

Glossary of terms

ABN	Australian Business Number - a single registrable numerical identifier for dealings with government departments and agencies
ABN - DSC	A digital certificate linked to an entity's ABN which identifies an individual with an associated entity that has an ABN
ABR	Australian Business Register - established under the *A New Tax System (Australian Business Number) Act* 1999 (Cth), this is a comprehensive register of information provided by businesses when they register for an ABN
ActiveX Control	Software technology developed by Microsoft that allows programmed capabilities or content to be delivered to Windows-based personal computers via the World Wide Web (notable for its lack of security controls; computer security experts discourage its use over the internet)
Address	An internet address or IP (internet protocol) address is a unique computer (host) location on the internet A web-page address - also called a Uniform Resource Locator (URL) – is expressed as the defining directory path to the file on a particular server An email address is the location of an email user (expressed as an email user name followed by the @ sign and then the user's server domain name
Address book	A feature of some email applications that stores names and email addresses in an accessible format (and one that can be exploited by some viruses which replicate by sending out copies of themselves via email)
Application	A self-contained program that performs a well-defined set of tasks under user control, as opposed to a system program (for example, web browsers, mail readers, and FTP clients are applications commonly used on the internet)
Archive file	A file that contains other files (usually compressed files), used to store files that are not used often or that may be downloaded from a file library by internet users
AFP	Australian Federal Police – established by the *Australian Federal Police Act* 1979 (Cth) as the agency with main responsibility for the investigation of crimes against Commonwealth laws, and with community policing responsibility for the Australian Capital Territory
AHTCC	Australian High Tech Crime Centre – hosted by AFP and established in 2004 as national agency dealing with technology-enabled crime investigations
AIC	Australian Institute of Criminology – an independent Commonwealth government body established by the *Criminology Research Act* 1971 (Cth)
ARPAnet	The original forerunner of the internet, designed for the United States military as a system able to withstand nuclear attack (though not human interference)
ASIC	Australian Securities and Investments Commission - an independent Commonwealth government body established by the *Australian Securities and Investments Commission Act* 1989 (Cth)
ATO	Australian Taxation Office – established as the administrative agency for Australian government revenue collection, headed by the Commissioner for Taxation under the *Taxation Administration Act* 1953 (Cth)
Attachment	A file that is embedded into an email message, and which requires a separate action to open (and which may also contain harmful code)
Audit trail	A chronological sequence of audit records containing evidence directly pertaining to and resulting from the execution of a business process or system function, which is useful for maintaining security and for recovering lost transactions. Audit trail may be admitted as evidence to establish or dispute the integrity or authenticity of an electronic record.
Authentication	A process of verifying the identity of a person or the identity of an entity (e.g. an individual).
B2B	Business to business – online communication between business entities
B2C	Business to consumer – online communication between business entities and consumers/ individuals
B2G	Business to government – online communication between business entities and government
Backdoor	An undocumented method of bypassing normal authentication or securing remote access to a computer
Backup	A copy of all information held on a computer in case something goes wrong with the original copy, produced as a result of either an automatic or manual command
Bandwidth	The amount of information or data that can be sent over a network connection in a given period of time, usually stated in bits per second (bps), kilobits per second (kbps), or megabits per second (mps)

BIOS	Basic input/output system – a program stored on the motherboard that controls the basic startup operations for the machine, which searches for the processor, memory, IDE (Integrated Drive Electronics) devices and ports, completes POST (Power on Self Test) checks and compares results with CMOS (Complementary Metal-Oxide Semi-Conductant), and assists the computer with booting of the computer.
Bit (binary digit)	A bit is either on or off and is represented by 1 or 0 (bits are put together to form a byte)
Bluetooth	A telecommunications industry standard which allows mobile phones, computers and personal digital assistants (PDAs) to connect using a short range wireless connection
Bookmarking	The process of storing the address of a website or internet document on your computer so that you can find it again easily
Boot	To start a computer, more frequently used when referring to the operating system that controls the computer.
Boot disk	A floppy disk that contains the files needed to start an operating system
Bot malware	Codes that typically takes advantage of system vulnerabilities and software bugs or hacker-installed backdoors that allow malicious code to be installed on computers without the owners' consent or knowledge.
Bot program	Codes that operate automatically as agents for a user or another program. The first bot program was probably Eggdrop, created by Jeff Fisher, which originated as a useful feature of internet relay chat (IRC) in the early 1990s. Early bot programs were designed to allow IRC operators to script automated responses to IRC activities.
Bots	Individual computers infected with bot malware – are then turned into zombies.
Botnet	A collection of software robots, or bots, which run autonomously and which the botnet's originator or botmaster can control remotely, usually through a means such as internet relay channel (IRC), and usually for nefarious purposes such as distributed denial of service attacks (DDoS)
Browser	A software application that displays and allows users to interact with text, images, and other information typically located on a web page at a website
Brute force attack	A tedious problem-solving technique which systematically enumerates all possible candidates for the solution and checking whether each candidate satisfies the problem's statement. For example, in a brute force attack, one defeats an encryption program by exhaustively working through all possible keys to decrypt a message
Buffer	An area of memory often referred to as the cache used to speed up access to devices. It is often used for temporary storage of data read from or waiting to be sent to a device such as a hard disk, CD-ROM, printer or tape drive.
Bulletin Board System (BBS)	A computer system equipped for network access that serves as an information and message passing centre for remote users, generally focused on special interests, such as science fiction, movies or computer software (may be free or fee-based)
Byte (short for binary term)	In most computer systems, a unit of data consisting of eight bits, which is the smallest addressable unit that can represent a single character, such as a letter, digit or punctuation mark
Cache	Browsed web pages are stored in the browser's cache directory on a PC's hard disk, so that when the page is revisited the browser can get it from the cache rather than the original server, saving time and the network the burden of additional traffic - two common types of cache are cache memory and disk cache
Carriage service	Defined in s7 of the *Telecommunications Act 1997* (Cth), and for telecommunications offences in the *Criminal Code Act 1995* (Cth), as 'a service for carrying communications by means of guided and/or unguided electromagnetic energy'
CDF	Channel data format, a system used to prepare information for webcasting
CD	Compact disc with a standard size of 700 megabyte
CD-R	Recordable compact disk – a disc to which data can be written but not erased
CD-ROM	A format and system for recording, storing and retrieving electronic information on a compact disk that is read using laser optics rather than magnetic means
CD-RW	Rewritable compact disc – a disc to which data can be written and erased
CERT	Computer Emergency Response Team (http://www.cert.org/)
Certification Authority (CA)	A body that generates, signs and issues Public Key Certificates which bind Subscribers to their Public Key
Chat	A form of interactive online communication that enables typed conversations to occur in real-time, with messages are instantaneously relayed to other members in the chat room

Chat room	Available through online services and some electronic bulletin boards, allowing the real-time exchange of messages between users of a particular system (may be open or secure chat rooms)
Checksum	A mathematical calculation applied to the contents of a packet before and after being sent (indicating errors in the transmission if the ‘before’ and ‘after’ calculation does not match)
Circuit board	A thin plate with chips, devices and other electronic components installed on the plate
CMOS	Complementary metal-oxide semi-conductant. This is a low-power memory chip that holds basic functionality data such as the power on password, time and date, drive search sequence and hard drive types. This is often confused with the BIOS chip. Basically the BIOS chip gets the computer up and running and compares what it finds against the settings saved the last time in the CMOS.
Communications data	Transmission of information from one computer/device to another
Compression	See file compression
Compromise	A violation (or suspected violation) of a system such that unauthorised disclosure of sensitive information may have occurred
Computer	A programmable machine that allows manipulation of data according to a pre-recorded list of instructions known as a program.
Configuration file	A file that contains initial configuration information/settings for a particular program
Cookie	A small message written in a user’s browser by a server when a website is connected to, enabling traffic to the website to be monitored (note that cookies can be turned off, but some websites will fail to appear properly without cookies activated and a message will appear on the screen with this information)
CPU	Central processing unit – the most powerful chip in the computer, the brain that performs all the computer’s arithmetic, logic and control functions
Cracker	A person who uses his or her skill to break into computer programs or DVDs protected by copyright and other protections such as key encryption systems, and who usually then makes the cracked software or DVD available for free or at a reduced cost (see also warez traders)
CRC	Cyclic redundancy check – a common technique for detecting data transmission errors
Cryptography	Cryptography is the expertise of scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (decryption) – this enables securing of private information sent through public networks by encrypting it in a way that makes it unreadable to anyone except the person or persons holding the mathematical key or knowledge to decrypt the information
Cybercrime	A general term encompassing crime committed by means of, directed at, or otherwise using or facilitated by, computers or associated technologies (also cyber crime or cyber-crime)
Cyberspace	The ‘place’ where computer networking hardware, network software, and people using them converge
Cyberstalking	The use of computers or associated technologies to stalk or harass a person
Cyberterrorism	The use of computers or associated technologies to commit an act of terrorism
Daemon	A program that runs in the background and provides system services on an ongoing, indefinite basis for one or more client applications, such as printing files on a shared printer
Database	Structured collection of data that can be accessed for uses including address links, invoicing information, statistical records, etc. (common database programs include Dbase, Paradox, Access)
Date and time stamps	A piece of data that enables the identification of the existence of a digital content at the particular date and time
Deleted files	Files sent to a PC’s recycle bin, with the consequent removal of the file’s root directory link (note, however, that depending on how the files are deleted, in many instances a forensic examiner is able to recover all or part of the original data)
Decryption	The reverse process to encryption
Denial of Service attack (DoS)	An attack aimed at specific websites by flooding a webserver with repeated messages, tying up the system and denying access to legitimate users – see also Distributed Denial of Service attack (DDoS)
Dictionary attack	A technique used to defeat an encryption or authentication mechanism by trying to determine its decryption key, password or passphrase by searching through predefined databases or dictionaries – see also brute force attack.
Digital certificate	An electronic document signed by the Certification Authority which identifies a Key Holder and the business entity he or she represents, binds the Key Holder to a Key Pair by specifying the Public Key of that Key Pair, and contains the information required by the Certificate Profile

Digital signature	An electronic signature created using a private signature key
Digital video (DV)	Video captured, manipulated and stored in a digital format
Directory	An entity in a file system which is used to organise files and/or files into a hierarchical structure
Disc space	The space on the web hosting a company's server/computers that a website's content is allowed to utilise
Disk	A medium for which data can be encoded and there are either magnetic disks or optical disks
Disk cache	A portion of memory set aside for temporarily holding information read from a disk
Distributed denial of service attack (DDoS)	A denial of service attack using multiple sources of messages, usually from a large number of computers connected to the internet
DNS	Domain Name System – identifies each computer as a network node on the internet using an internet protocol address system to translate from domain names to IP numbers and vice-versa
DNS server	The facility that operates the DNS to allow connection between computers on the internet
DVD	Digital Versatile Disk - similar in appearance to a compact disk, but can store larger amounts of data including video
Dynamic IP address	Dynamic IP address is issued to identify non-permanent devices that takes place at the moment when needed rather than in advance (see also IP address)
Electronic Funds Transfer (EFT)	The paperless act of performing financial transaction electronically through a computer network
Electronic signature	A data element associated with a message, which identifies a person and indicates his or her approval of the contents of the message
Email (or e-mail)	Electronic mail – emails come in two parts, the body and the header
Email header	Normal header information gives the recipient details of time, date, sender (automatically added) and subject (as typed by sender), while extended headers include information added by email programs and transmitting devices which may show other information about the sender enabling tracing to an individual computer on the internet
Email server	A mail transfer agent (MTA) or a system of MTAs that enable routing of electronic mail (email) and act as a server, by storing email and supporting client access
EnCase	Commercially available forensic software product, produced by Guidance Software
Encryption	The process of scrambling, or encoding, information in an effort to guarantee that only the intended recipient can read the information
Expansion board	A printed circuit board that can be inserted into a computer to add capabilities such as increased memory
Expert evidence/expert opinion	Evidence in the form of an expert's opinion which is admitted in court proceedings despite the general prohibition on opinion evidence, must be wholly or substantially based on the witness' training, study or experience (e.g. see s79 of the *Evidence Act 1995* (Cth))
FAQ	Frequently asked questions – many websites have such a list of questions and answers
File compression	A technology that reduces the size of a file, saving both time and bandwidth in transmission (e.g. WinZip and UNIX compress are compression programs)
File extension	Part of the name of a file that determines its type and function: examples include .doc, .exe and .bat
File sharing program	Computer codings that enable electronic transfer of files from one computer to another over the internet, over a smaller Intranet, or across simple networks
File signature	(See Digital signature)
Filtering	Internet filtering systems prevent or block user's access to unsuitable material.
Firewall	A network security system used to restrict external and internal traffic
Floppy disk	These are square, flat disks that hold information magnetically, with two main types: 3 ½inch (in a stiff case) and 5 ¼inch (flexible and more easily damaged)
Folder	An object containing multiple documents and are used to organize information (See Directory)
Forensic computer examiner	A specialist who examines computer systems to determine whether they are or have been used for illegal or unauthorized activities
Free space	Can contain clusters that are not currently used by the operating system but contain deleted files or data
Gigabyte (GB)	A measure of memory capacity, roughly one thousand megabytes or a billion bytes (1 gigabyte = 1024 megabytes)
Google	A particularly popular search engine: http://www.google.com/

Hacker	A person who uses his or her skill to break into computer programs, obtaining unauthorised access to data and/or the functionality of a computer and systems to which it is connected
Hacking	The activity of a hacker, which may be done with honest motives (e.g. testing a system's security) or with dishonest aims (e.g. obtaining confidential information or causing damage to a computer or system)
Hard disk/Hard drive	The hard disk or hard drive is usually inside the personal computer and stores information in the same way as floppy disks but can hold far more
Hardware	The physical parts of a computer – those that can be kicked
Hash	A mathematical algorithm that creates a small digital fingerprint from any kind of data
Host machine	In forensic examination, a host machine is one which is used to accept a target hard drive for the purpose of forensically processing it
HTML	Hypertext markup language (a subset of the Standard Generalized Markup Language (SGML) first invented to display legal texts and now the world standard for large documentation projects) - the text markup language used to insert tags which allow a web browser to correctly display a hypertext document (HTML1, HTML +, HTML 2 and HTML 3 are versions of HTML in use)
HTTP	Hypertext Transfer Protocol – An internet protocol that manages the transfer of hyper-text (web pages) and multimedia documents over the internet
HTTPD	Hypertext Transfer Protocol Daemon – a computer program which manages the transfer of hypertext and multimedia documents over the internet
Hypertext	Text which contains links to other text – internet web pages are an example of documents that contain such links.
Hypermedia	Electronic documents which combine hypertext links and multimedia elements
IT/ICT	Information and Information technology (IT) or information and communications technology (ICT) is the technology required for information processing – in particular the use of electronic computers and computer software to convert, store, protect, process, transmit, and retrieve information
Identity theft/identity fraud	The act of surreptitiously obtaining identifying details of a person (by means including hacking, phishing, credit card skimming, etc.) and misusing this in criminal ways including fraudulent misrepresentation
IDS	Intrusion detection system (IDS) is designed to detect malicious network traffic and to monitor computer usage that cannot usually be detected by a conventional firewall
Imaging	The process of obtaining all of the data present on storage media, whether active data or in free space, to allow it to be examined by a forensic examiner
Instant messaging	A form of electronic communication that is carried out in real-time between two or more people over a network such as the internet.
Internet	The collective electronic network of computers and computer networks which are inter-connected throughout the world – started with the ARPAnet
Internet Relay Chat (IRC)	A virtual meeting place where people from anywhere in the world can meet and talk online about a diversity of human interests, ideas and issues
IP address	A unique number that is used for identification by devices to communicate with each other on a computer network utilising the internet protocol (IP) standard
IP spoofing	Creation of internet protocol (IP) packets with a forged source IP address
Internet Service Provider (ISP)	A business or organisation that offers fee-paying or subscribed users access to the internet and related services – most telecommunications operators are ISPs and provide services such as internet transit, domain name registration and hosting, dial-up access, leased line access and co-location
IPPs	Information Privacy Principles - the principles set out in s 14 of the Privacy Act 1988 (Cth)
IPRs	Intellectual Property Rights – including copyright and neighbouring rights, patents, plant breeder's rights (PBR), registered and unregistered trademarks, registered designs, confidential information (including trade secrets), circuit layouts, and other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields, protected by a range of legislation and common law actions
Java	An object-oriented programming language developed at Sun Microsystems in the early 1990s
Jaz	A high capacity removable hard disk system
Jumper	A conductor, consisting of a plastic plug that fits over a pair of protruding pins, is generally used to set up or adjust printed circuit boards
Keyboard	A device with many keys (usually marked with the letters of the alphabet, the numerical digits, and various extra keys) that allows user to input data into a computer

Keystroke logger (monitor)	A diagnostic computer program that is to capture the user's keystrokes
Kilobyte (KB)	A measure of memory capacity (1 kilobyte = 1024 bytes)
Linux	An operating system initially designed to provide users with a free alternative to Unix and Microsoft. Because of its many free distribution versions this OS is now used in a wide range of commercial products and is typically seen in servers and network architecture rather than at user level. Linux is a favoured tool of experienced hackers as it allows them to control to a very high degree all interaction from their machine to the victim machine. It also allows them to circumvent security measures in DOS based systems with relative ease
Logic bomb	A piece of malicious code, intentionally inserted into some computer system, that sets off a malicious function when specified conditions are met
Login	The process of gaining access to a computer system by entering the required identification, such as a password
Macro	A shortcut, such as a symbol, name or key, representing a list of commands, actions, or keystrokes
Macro virus	A virus attached to instructions (called macros) which are executed automatically when a document is opened
Magnetic media	A disk, tape, cartridge, diskette, or cassette that is used to store data magnetically.
Malware	Short for malicious software – software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse
MD5 hash	A mathematical algorithm created in 1991 by Professor Ronald Rivest that is used to create digital signatures of storage media such as a computer hard drive (when the algorithm is applied to a hard drive then it creates a unique value, so that changing the data on the disk in any way will change the MD5 value)
Megabyte (MB)	A measure of memory capacity (1 megabyte = 1024 kilobytes)
Memory	Often used to denote random access memory (RAM), which is the electronic holding place for instructions and data that a computer's microprocessor can reach quickly (RAM is located on one or more microchips installed in a computer)
Meta data	Data that is used to describe other data
Microsoft Windows	A family of operating systems developed by Microsoft
Modem	Modulator/demodulator. A device that connects a computer to a data transmission line (typically a telephone line). Most people use modems that transfer data at speeds ranging from 1200 bits per second (bps) to 56 Kbps. There are also modems providing higher speeds and supporting other media. These are used for special purposes – for example to connect a large local network to its network provider over a leased line
Monitor	The screen on which a PC displays information
Mouse	A device that, when moved relays speed and direction to the computer, usually moving a desktop pointer on the screen
MS-DOS	Microsoft DISK Operating System – the operating system marketed by Microsoft, the most common operating system in use on desktop PCs, which automatically loads into the memory of a computer when the computer is switched on
Multimedia	Electronic documents which contain text, sound, graphics and video elements that are all capable of being displayed to the user
Newsgroups	A repository that is used for messages posted from many users at different locations
NTFS	New Technology File System (NTFS) is the standard file system used in Windows NT, Windows 2000, Windows XP, Windows Server 2003 and Windows Vista
Open source	A software development model that allows public assess to the production and development of programs (see http://www.opensource.org/)
Operating system (OS)	This software is usually loaded into the computer memory upon switching the machine on and is a prerequisite for the operation of any other software
ORB	A high-capacity removable hard disk system. ORB drives use magnetoresistive (MR) read/write head technology
Packet	A formatted block of information carried by a computer network
Packet filtering	A means of controlling access to a computer network by analysing the incoming and outgoing packets and letting them pass or halting them based on the IP addresses of the source and destination
Packet sniffer	A program/device that monitors data packets travelling over a computer network
Partition	Dividing a computer's hard disk into several independent parts or dividing a computer into several independent virtual computers

Password	A word, phrase or combination of keystrokes used as a security measure to limit access to computers or software (many people choose an easy-to-remember sequence such as 123456 or their own name, making the hacker's job far easier)
Payload	Payload of a virus or worm is any action it is programmed to take other than merely spreading itself
PCMCIA cards	Similar in size to credit cards, but thicker, which are inserted into slots in a laptop or palm-held computer and provide many functions not normally available to the machine (modems, adapters, hard disks)
Personal computer (PC)	A term commonly used to describe IBM and compatible computers, but more generally, any computer useable by one person at a time
Personal organiser or personal digital assistant (PDA)	These are pocket-sized machines usually holding phone and address lists and diaries as well as other information, making them an attractive target for theft (both for the device and the information contained)
Pharming	Seeks to obtain confidential/sensitive information through domain spoofing.
Phishing	Assuming the identity of a legitimate organisation or website using forged email or fraudulent websites to convince others to provide information – usually personal financial, such as credit card numbers, account user names and passwords, social security numbers – for the purpose of using it to commit fraud
Phreaking	Exploiting telephone systems or the Public Switched Telephone Network (PSTN) for the purposes of making free phone calls
Pirate software	Software that has been illegally copied
Pop up	A form of online advertising and works when certain websites are opened, a new web browser window displaying the advertisements will be opened
Port	This is where information goes into or out of a computer, such as the serial port on a personal computer where a modem is connected
Port scanner	A program that is designed to search a network host for open ports
Post Office Protocol (POP)	An application-layer internet standard protocol, that is used by email client machines to retrieve email from a remote server over a TCP/IP connection
Protocol	A set of rules governing electronic communication between computer devices
Proxy server	A dedicated computer within a computer network service that allows other client machines to make indirect network connections to other network services
Public domain software	Free programs, also known as freeware, offered as an alternative to commercial products (for example, the Linux operating system)
Public key infrastructure (PKI)	A setting that allows a trusted third party to vet and vouch for user's identity which allows binding of users to public keys. The latter is typically embedded in digital certificates
Query	To search or ask. In particular, to request information on a search engine, index directory or database
RAM	Random access memory is the PC's short-term memory. It provides working space for the PC to work with data. Information stored in the RAM is lost when the PC is turned off
Remote access	The ability to connect to a network from a distant location, usually requiring a computer, a modem and remote-access software to allow the computer to connect to the network over a public communications network (such as a phone or cable network)
Removable media	Items, e.g. floppy disks, CDs, DVDs, cartridges, tape that store data and can be removed easily
Removable media cards	Small-sized data storage media which are more commonly found in other digital devices such as cameras, PDAs and music players. They can also be used for the storage of normal data files which can be accessed and written to by computers. There are a number of these: smartmedia, compact flash, SD expansion card, Ultra-compact flash, memory stick, multimedia card. The cards are non-volatile they retain their data when power to the device is stopped and they can be exchanged between devices
Root kit	Cloaking technologies that are usually employed by other malware programs to abuse compromised systems by hiding files, registry keys and other operating system objects from diagnostic, anti-virus and security programs
Server	A dedicated computer that provides services to other computers or the software that runs on it
Shareware	Software that is distributed free on a trial basis with the understanding that if it si used beyond the trial period, the user will pay. Some shareware versions are programmed with a built-in expiration date
Slack space	The unused space in a disk cluster. The DOS and Windows file systems use fixed-size clusters. Even if the actual data being stored requires less storage that the cluster size, an entire cluster is reserved for the file. The unused space is called the slack space

Smartcard	Plastic cards, typically with an electronic chip embedded that contain electronic value tokens. Such value is disposable at both physical retail outlets and online shopping locations
Software	The pre-written programs designed to assist in the performance of a specific task such as network management, web development, file management, word processing, accounting or inventory management
Spam	Junk mail (such as commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services) delivered by email or text messages, costing the sender very little to send as most of the costs are paid for by the recipient or the carriers rather than by the sender, regulated in Australia (with heavy civil penalties for spamming) by the *Spam Act 2003* (Cth)
Spamming	The act of flooding the internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it (see spam)
Spim	An alternative name for spam using instant messaging
Spyware	Any software that covertly gathers user information through the user's internet connection without his or her knowledge, usually for advertising purposes – spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet, which, once installed, monitors user activity on the internet and transmits that information in the background to someone else, and may also gather information about email addresses, passwords and credit card numbers
Steganography	An information hiding technique that usually embeds messages within other, seemingly harmless messages or files
Streaming	One-way (either point-to-point or broadcast to multiple receivers) transmission of video and audio content over the internet or advanced wideband wireless networks
System unit	Usually the largest part of a PC, the system unit is a box that contains the major components – it has the drives at the front and the ports for connecting to the keyboard, mouse, printer and other devices at the back
Tape	A long strip of magnetic-coated plastic, usually held in cartridges (similar in appearance to video, audio or camcorder tapes) but can also be held on spools (similar to reel-to-reel audio tape), used to record computer data, usually a back-up of the information on the computer
TCP/IP	A set of protocols covering the network and transport layers of the seven-layer Open Systems Interconnection (OSI) network model. TCP/IP was developed during a 15-year period under the auspices of the U.S. Department of Defense. It has become a dominant standard in enterprise networking, particularly at higher-level OSI layers over ethernet networks
Terabyte (TB)	A measure of memory capacity, roughly one thousand gigabytes or a billion kilobytes (1 terabyte = 1024 gigabytes)
Terminal	A computer terminal is a device, such as a combination of keyboard and display screen, allowing the user to communicate with a computer or computer system
Thumbdrive	A form of USB flash drives that allows portable storage of data
Thumbnail	Reduced-size versions of digital pictures
Tracert (traceroute)	A computer network tool that is used to determine the network route taken by data packets across an IP network
Traffic data	(See Data packets)
Trojan horse	A type of malicious program used to establish remote access to a victim's machine, typically disguised as innocent attachments to email but when executed install software that allows the attacker to remotely access and control some or all of the primary functions of the victim's computer. Trojans can also be remotely installed by exploiting faulty code, so that the victim may only need to visit a website for their computer to become infected
Trojan horse defence	A defence argument sometimes raised to put forward an alternative explanation for the presence of illegal content or incriminating data on a computer, relying on the hypothesis of a third party attack by means of malicious code
Unallocated file space	Unallocated file space (also known as free space) is the unused portion of the hard drive and often potentially contains intact files, remnants of files and subdirectories and temporary files which were transparently created and deleted by computer applications and also the operating system
Unix	A popular operating system, used mainly on larger multi user systems (Unix-based systems control the majority of primary functions on the internet and represent 50% of the web servers in use today)
Unauthorised access, modification or impairment	An element of several computer offences under the *Criminal Code Act 1995* (Cth) and similar legislation in the states and territories, where access to, modification or impairment of data or electronic communications is unauthorised if 'the person is not entitled to cause that access, modification or impairment' (s476.2)

URL	Uniform Resource Locator – the global address of documents or web pages on the World Wide Web, with the first part of the URL (most often http://) indicating the protocol to be used and the remaining part (such as www.organisation.au) identifying the webpage to be displayed
USB storage devices	Small storage devices accessed using a computer's USB ports that allow the storage of large volumes of data files and which can be easily removed, transported and concealed (also called datakeys and thumbdrives)
Username	The unique identifier for each user on a network, usually required with a unique password for logging on
Usenet	The computer network which carries newsgroups – arranged in hierarchies based loosely on subject matter
Video backer	A program that allows computer data to be backed up to a standard video. When viewed the data is presented as a series of dots and dashes
Video conferencing	A live connection between people in separate locations for the purpose of communication usually involving audio and often text as well as video
Virus	A piece of programming code which is inserted into other programming code for the purpose of causing some unexpected and (for the victim) usually undesirable event, ranging from relatively harmless screen messages to highly destructive programs that erase or alter data – viruses can be transmitted by downloading programs from other sites or from portable storage media, and may include self-replicating functions and mechanisms for further distribution (e.g. via address books attached to email facilities)
Voice Over Internet Protocol (VOIP)	A technology that allows users to make telephone calls over the internet instead of the traditional analog phone line
War driving	A technique used to search for Wi-Fi wireless networks using a Wi-Fi-equipped computer in a moving vehicle
Webcam	A webcam is a camera connected to the internet that can be used to stream moving images. (A live picture, or snapshot is uploaded to a website from the camera at regular intervals, typically every few minutes for a webcam located at a fixed location such as a city centre.)
Weblog (blog)	A form of online diary or journal, consisting usually of short, frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page (blogs may also contain photos, images, sound, archives and related links and can incorporate comments from visitors)
Web server	A server that runs services which process requests for web content – see also server
Website	A collection of files accessed through a web address, covering a particular theme or subject, and managed by a particular person or organization. Its opening page is called a home page. A Website resides on servers connected to the internet and is able to format and send information requested by worldwide users 24 hours a day, seven days a week. Websites typically use Hypertext markup language (HTML) to format and present information and to provide navigational facilities that make it easy for the user to move within the site and around the Web.
Whois	A widely used (domain name lookup) technique to query a domain name database to determine the owner of a domain name or an IP address on the internet
Windows 95, Windows 98, Windows ME etc.	Operating system marketed by Microsoft for use on desktop PCs
Wired equivalent privacy (WEP)	A feature used to encrypt and decrypt data signals transmitted between Wireless LAN (WLAN) devices. An optional 802.11 feature (e.g. 802.11), WEP provides data confidentiality equivalent to that of a wired LAN that does not employ advanced cryptographic techniques to enhance privacy. WEP makes WLAN links as secure as wired links.
Wireless data communication	A form of communication that uses the radio spectrum rather than a physical medium. It may carry analog or digital signals and may be used on LANs or WANs in one or two-way networks.
Windows NT	Operating system from Microsoft aimed at the business market. Multiple layers of security are available on this system.
Word processor	Used for typing letters, reports and documents - common programs are Wordstar, Wordperfect, Microsoft Word
World Wide Web (WWW or W3)	The name given to the collection of computers which serve information in hypertext format to the internet – invented by Dr Tim Berners-Lee, at the European Center for Nuclear Research (CERN), who wrote the first hypertext transfer protocol daemon (HTTPD) and the first hypertext markup language (HTML) browser, as a way to allow nuclear physicists to exchange working papers over the computer networks
Worm	Like a virus but is capable of moving from computer to computer over a network without being carried by another program

Wireless network card	An expansion card present in a computer that allows cordless connection using radio signals between that computer and other devices on a computer network, replacing traditional network cables
Yahoo!	A popular search engine: http://www.yahoo.com/
Zip drive/disk	A 3.5 inch removable disk drive. The drive is usually bundled with software that can catalogue disks and lock files for security.
Zip	A popular data compression format. Files that have been compressed with Zip format are called zip files and usually end with a .zip extension.
Zombie (see also bot and botnet)	A recently introduced term to denote a computer that has had some of its functions brought under remote control, usually without the owner's knowledge or consent, by means of a virus or other malicious software. An army of zombies forms a botnet.