Chapter 2

Crime in Cyberspace

What is cybercrime?

2.1 The Committee notes that there is no statutory definition of cybercrime.

2.2 The expression 'cybercrime' is a product of the expansion in communications technology which has accelerated over the last twenty five years. A number of definitions of cybercrime was provided to the Committee. The Attorney General's Department defined it as:

> a term that encompasses a variety of offences associated with the use of information and communication technology. The use of the term Cybercrime is synonymous with the term electronic crime (e-crime).[1]

2.3 From the Australian Bankers' Association comes this definition:

> A cybercrime is any crime effected or progressed using a public or private telecommunications service.[2]

2.4 The Australian Crime Commission (ACC) observed that the expressions e–crime, Computer Crime, High Tech Crime, and Cybercrime all refer to the same phenomenon and quotes the definition of e-crime as used by the Australian Centre for Police Research:

> [E-crime includes] offences where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence. [3]

2.5 However, in evidence, the Australian High Tech Crime Centre (AHTCC) distinguished between a definition which focuses on the Internet and one which also includes a number of other technological features

> … we are not concentrating just on the Internet – and cyber is usually referred to as the Internet. We are looking at the misuse of technology in a more holistic sense. The danger is that we will miss other exploits or other criminal activities that fall outside the strict definition of the Internet … . We do not want to limit ourselves to just the Internet, while recognising that the Internet will form the backbone of a whole range of those activities – even things like telephony, with the move to IP telephone systems rather

---

1 Attorney-General's Department, Submission no 21, p.2

2 Australian Bankers' Association, Submission no 19, p.6

3 Australian Crime Commission, Submission no 23, p.6

> than switch systems, are becoming part of the Internet. That is the reason for drawing that distinction.[4]

2.6 The Committee observed that the AHTCC's perspective is not static; it accommodates emerging communications technologies as well as those which are current. The possibilities of mobile phone technology are immense, and the AHTCC's interpretation allows for monitoring developing technology as well as meeting the challenges of that which is current.

A means to an offence

2.7 The definition used by the ACC identifies three kinds of offences which involve the use of communications technology, including the Internet.

2.8 The first kind is an offence which is committed using the technology; effectively it is a conventional crime such as fraud which is committed by technological means.

Computers as targets

2.9 The second kind involves offences which target the computers themselves, and seek to destroy or alter information or data held in them, sometimes with a view to interfering in the processes which that data governs. An example would be an attempt to disrupt a city's water supply by interfering with the computers which control it. The interference can be exercised by a number of means including by hackers, worms, viruses and Trojans.

Hackers

2.10 Hackers are people with sufficient technical ability to gain access to another person's computer or to a network through the use of stolen passwords, or interference technology which provides access to networks and individual computers. It is a recognised and for some, an accepted form of computer activity.

2.11 Symantec's evidence described three different hacking groups:

> The first group are … young kids, 15 to 21 years old, who download the latest hacking tools straight off a web site. If you … go into … any search engine, type in 'hacking tools' and hit return, a plethora of sites come up that will give you the ability to generate your own malicious codes, worms, viruses, hack attacks ... Most of that is filtered out as noise by the technology … They are known vulnerabilities and they are known attacks, so they are fairly easy to block.
>
> The second group would be politically motivated organisations that are attempting to hack into specific countries, for example, organisations that are anti global trade and that sort of thing. You see attacks on high-profile

4 *Committee Hansard,* 21 July 2003 p.24

> commercial organisations launched by special interest groups of that nature on occasions. The final group is … those that are a little more talented in what they do. They … are specifically after personal gain. They … tend to launch the attacks that are not as high profile because you tend not to hear about them. They … are trying to steal credit card information or deploy keystroke loggers without people knowing about it. These things are not designed to bring down infrastructure … or hack into web sites … they are trying to specifically pick up their own information without people knowing. They are … predominantly male, predominantly 15 to 35 years of age.[5]

Worms, viruses and trojans

2.12 The terms 'worm' and 'virus' in relation to computers, are often used interchangeably. However, there are differences between them. A computer worm is a self-replicating computer program, which unlike the virus does not need to attach itself to another program in order to propagate itself. A worm can delete files, or send email documents.

2.13 A virus is a piece of program code, so called because like a biological virus it copies itself and then attaches to a 'host' – another computer program. That program can be another operating system which then transfers the virus to other computers, damaging all in its wake. Viruses can be destructive by altering files or erasing information from disks. More seriously they can allow others to gain access to a person's computer without authorisation.

2.14 Trojans are a stand alone program which does not attach to another program; it does not move from computer to computer on its own, but must be transferred intentionally, such as through email. Trojans are usually malicious: a person can email it with an unremarkable filename and attach a message which, when opened might alter or delete files on the machine, or access emails. As they are transferred deliberately, they generally do not infect other programs and are usually easily deleted.[6]

2.15 Viruses and worms first appeared in the 1980's and Trojans in the mid 70's. With the increasing availability of technology, the opportunities for interference have also multiplied.

Computers as storage

2.16 The third category identified in the definition used by the ACC includes offences in which the computer is used as storage for information about an offence, for example a drug offence in which supply records are kept on computer.

---

5 *Committee Hansard*, 18 July 2003, p.74

6 The definitions of 'worm', 'virus' and 'Trojan' are based on material from the online 'Wikipedia' at: http://www.wikipedia.org.

Crime and the internet

Internet access

2.17 The submission from the Australian Broadcasting Authority (the ABA) notes that the most common Internet access is through a personal computer and a phone line.[7] However, the Authority anticipates that emerging technologies will provide the capacity to access the Internet and other online services using a range of devices, including mobile devices.

2.18 The Australian Bureau of Statistics notes that as at 31 March 2003 there are 4,417,000 household Internet subscribers in Australia. This has increased from 3,486,000 in the March quarter of 2001.[8] The market for those intent on using the Internet for criminal purposes has increased by 37 % in only two years.

2.19 The growth of technology has resulted in a parallel growth of associated criminal activity. Of some concern to the Committee were reports concerning paedophilia, and the ease with which children could be contacted by paedophiles through communications technology. The Committee was also concerned at the extent of the misuse of card technology and the Internet. Advanced telecommunications technology can also threaten the viability of utilities such as electricity and water, and because the Internet knows no international boundaries, this can be achieved from an area remote from the affected facility.

2.20 The Committee noted that the Internet has features which favour criminal activity. They include:

- unregulated establishment of, and access to Internet and email sites;
- anonymity; and
- lack of security and public awareness.

Unregulated establishment and access

2.21 Internet Service Providers are not required to be licensed, and are not regulated except by voluntary codes of conduct. Free email providers such as AOL, Yahoo and Hotmail (all of which operate from outside Australia) require minimal information from the user, making the detection of offenders difficult.

2.22 It is also possible to falsify email software to make an email appear to come from a particular source, but in reality be sent by a third party.[9] One of the most familiar effects of unregulated email is SPAM; these are unwanted emails which may be used to harass, to acquire funds fraudulently (the 'Nigerian' letters in which

---

7 Australian Broadcasting Authority, Submission no 15, p.16

8 Australian Bureau of Statistics publication 8253.0, *Internet Activity*, 1 Sept 2003.

9 PricewaterhouseCoopers, Submission no 12a, pp.25-26

recipients were asked for bank account numbers is an example) or to distribute pornography.

Anonymity

2.23 The Committee noted that Internet and computer criminal activity is supported by the anonymity of the environment. In email, free email services allow the creation of as many different email identities as the user wishes, without any useful information about the identity of that person. In evidence Mr. Gregory Melick observed:

> A short-term fix which would make life a lot easier would be to do away with free Internet accounts such as AOL and Hotmail … because if Internet accounts are not free, people have to pay by credit card, and the vast majority of people who use credit cards have provided appropriate information when obtaining the credit cards and that gives law enforcement some starting point.[10]

2.24 Mr Melick indicated that as far back as 1996 (when there were only 600,000 Internet users in Australia: there are now 7 million) that everybody who used an Internet account should have to go through a 100-point check, the same as if opening a bank account:

> Industry thought the idea was laughable and it had amazing problems, because if we do it in isolation it does not do much about the people in the rest of the world who have access to accounts over there. … In 2000 the United Kingdom had six million [Internet users]; in 2002 it had 10 million. In the United States alone from 1996 to 1997 – that is, from the beginning of 1996 to the end of 1997 – Internet users went from 40 to 100 million … if one does not start doing something about it sooner rather than later we are going to have further problems down the line. France … about two years ago … enacted such provisions.[11]

2.25 The 100 point check system has some drawbacks as the Australian Bankers' Association pointed out.[12] The 100 point check requires provision of original documents, and the increased ability to copy and forge documents easily undermines the integrity of the system, although it is clearly an improvement on no system at all.

Chat Rooms

2.26 Chat Rooms on the Internet were described during the Inquiry as being similar to a conference call on a telephone.[13] Chat rooms use Internet technology to allow a group of people with similar interests to communicate using the one Internet location.

---

10 *Committee Hansard*, 21 July 2003, p.28

11 *Committee Hansard,* 21 July 2003, p. 29

12 *Committee Hansard,* 18 July 2003, p. 45

13 *Committee Hansard,* 18 July 2003, p.15

Access is readily available although in some cases a password might be required. In chat rooms, the participants may also assume identities which are untraceable, or false, which is why these are an ideal environment for paedophiles.

2.27 Chat rooms are an instant form of communication – unlike email which is relayed, and then read. The danger inherent in a chat room is its immediacy and somewhat clandestine nature. Children in particular, can be using chat rooms without their parents being any the wiser – the activity would simply appear in the same way as any typing or entering of text. Although some witnesses indicated it has been possible for police to enter chat rooms to monitor proceedings, gathering evidence in the environment is difficult, time consuming, and may not be cost effective.

2.28 In evidence Symantec Australia indicated that the technological barriers to monitoring chat rooms are not insurmountable:

> If you look at the whole instant messaging or chat room space, … there are a lot of third party solutions out there which you can bolt on to existing instant messaging and chat room technologies to record the conversations. It is just a matter of going out and finding the right bits that fit together and knowing how they work. I do not see that there are any real technology barriers there. It is just an extension of email, which we are all used to and is logged and recorded.[14]

2.29 However, Symantec also informed the Inquiry that there may be some barriers to this because of the increasing use of encryption, which is resource-intensive to decode. The Committee notes from this that although the technology may be available, it may not be feasible to use it for monitoring chat rooms.

Other devices

2.30 There are also devices which can mask the source of information, making it appear that the content is actually from another source.

Security and public awareness

2.31 The evidence showed there are two areas of vulnerability for users of the Internet. One is the potential for access by children to unsuitable content and to features such as chat rooms, and the other is a lack of general awareness of the need to secure a computer. This protects the user not only from nuisance email but also from malicious content (including viruses) and from hacking to obtain details such as Internet banking and on-line shopping transactions.

2.32 The Committee was advised by a number of submitters and witnesses that many parents rely on software filtering programs to protect their children from unsuitable content. These are of varying degrees of usefulness, as the filter tends to eliminate material which appears to be objectionable but which is not. Filters can also

---

14 *Committee Hansard,* 18 July 2003, p.75

do the opposite, and fail to filter very much content at all. There is nothing available at present which will restrict access to sites such as chat rooms.

2.33 Many consumers install virus protection, but do not update it. 'Firewall' programs are available (and are often supplied with computer packages) to assist with blocking malicious content, but consumers either don't install or don't update them, or are unaware that this kind of protection is available.

2.34 The consequences of not having such protection can be serious, as they can be easily attacked by computer hackers, worms and viruses. The virus protection packages are a small expense compared to the havoc which can be caused to personal records, as well as major networks. Even keeping virus and firewall protection up to date does not guarantee full immunity, but most anti virus software companies are able to advise consumers of the latest potential dangers, and the appropriate action to take to minimise damage.

Legislation and law enforcement

2.35 The Attorney General's Department notes in its submission to the Inquiry, there is no single Australian law enforcement or policy body which has responsibility for cybercrime matters. Further, cybercrime enforcement is the responsibility of a diverse group of organisations which include law enforcement, regulatory authorities and research bodies:

> The responsibilities of these organisations are diverse, and in most cases Cybercrime forms only a portion of their work. Each of these entities has different roles ranging from the development and coordination of policy, to the policing and prosecution of crime.[15]

2.36 The submission also observes that there are increasingly significant roles being undertaken by the ACC, and the AHTCC.

The role of the ACC and AHTCC in cybercrime

The ACC

2.37 The *Australian Crime Commission Act 2002* (the Act) sets out the organisation's function. Section 7A (see Appendix 1) sets out the details of its work which includes:

- the collection and analysis of criminal information and intelligence;
- investigative work authorised by the ACC Board on matters relating to 'federally relevant criminal activity'; and
- advising the Board on criminal intelligence priorities and providing strategic criminal intelligence assessments.

---

15 Submission no. 21, p. 17

The Australian High–Tech Crime Centre

2.38 The AHTCC is established as part of the Australian Federal Police. The *Australian Federal Police Act 1979* (the AFP Act) sets out the AFP's role. The relevant sections are set out in section 8 of the AFP Act (see Appendix 1) and include the provision of police services. Police services are defined in the AFP Act as:

> police services include services by way of the prevention of crime and the protection of persons from injury or death, and property from damage, whether arising from criminal acts or otherwise.

2.39 The role of the ACC in relation to cybercrime is similar to the other areas of serious and organised crime mentioned in section 4 of the ACC Act. The ACC is responsive to events which have occurred rather than to those which might occur. Its work is that of a processor of information, an intelligence gatherer, and an operational body which acts on the information and intelligence.

2.40 The AHTCC is sponsored by the AFP and its policing role includes the co-ordination of Australian law enforcement agencies to combat serious crime involving complex technology.[16] This includes:

- providing a national coordinated approach to combating serious, complex and multi-jurisdictional high tech crimes, especially those beyond the capability of single jurisdictions;
- assisting in improving the capacity of all jurisdictions to deal with high tech crime; and
- supporting efforts to protect the National Information Infrastructure.

2.41 The Committee sees the AHTCC's work complementing that of the ACC: the ACC may be said to be primarily an operational organisation, focused on a number of areas of serious and organised crime. The AHTCC is a co-ordinating body which of necessity must have research and analysis resources, in order to provide the support to the state and territory bodies which are its constituents. It is in a position to provide comprehensive information on its particular area of expertise: high tech crime.

2.42 However, in the Committee's view the inter-jurisdictional and international nature of cybercrime demands not only a co-ordinated and unified national strategy but one placed in the international context.

2.43 The Committee notes that much unacceptable Internet activity originates outside Australia, which makes detection and prosecution difficult without some form of international co-operative detection and prosecution system. Tracing and eliminating cybercrime requires a legislative framework that is consistent both domestically and internationally.

---

16 'What is the AHTCC?', http://www.ahtcc.gov.au/

2.44 The ABA, for example, indicated in its submission that a significant proportion of child pornography is produced and/or hosted in Russia and some other Eastern European nations. The Australian Federal Police (AFP) has advised the ABA that 'authorities in these jurisdictions have not attached a high priority to investigating such matters.'[17] The Committee shares the ABA's concern; on an international level it is clear that the commitment to developing a framework for detection and enforcement cannot be assumed, although there are initiatives through The United Nations (Resolution of the General Assembly no 55/63 'Combating the Criminal Misuse of Information Technologies' – see extract at Appendix 4) and, as the Committee was informed by Mr Orlowski, APEC.[18]

2.45 The UN resolution includes recommendations which if implemented would establish a framework for international co-operation creating a responsibility for states to ensure that the misuse of technology can be appropriately investigated, prosecuted and penalised. It also includes the recommendation that the 'general public should be made aware of the need to prevent and combat the criminal misuse of information technologies'.[19]

2.46 In evidence, Mr Orlowski told the Committee of APEC projects following the UN resolution which are designed to assist developing economies:

> [APEC] have done a report on what economies [countries] are doing to implement the United Nations General Assembly resolution. ... At the moment … we are running a workshop to assist developing economies, in particular, to develop cybercrime legislation. At the last count, we had 120 representatives nominated for that workshop, which is quite a large number by APEC standards. That will be followed up by in-country training provided by the United States Department of Justice. They will go to the different economies and work with them to try to get that legislation at least underway by October 2003.[20]

2.47 The Australian arrangements for the areas of UN concern are contained in legislation and in particular, mutual assistance arrangements. The Attorney General's Department submission outlined these.[21] They include the Mutual Assistance Unit in the Attorney-General's Department. The unit has the following functions:

---

17 Submission no 15, p.12

18 APEC is the acronym for Asia Pacific Economic Co-operation. It is a 21 member organisation established in 1989 to further enhance economic growth and prosperity for the region and to strengthen the Asia Pacific community. (http://www.apecsec.org.sg/apec/aboutapec.html)

19 Resolution no 55/63 of the UN General Assembly, 81ST Plenary Meeting, 4 December 2000 (http://ods-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17)

20 *Committee Hansard*, 17 July 2003, p.2

21 Submission no.21, p.15

- Making requests for assistance in criminal matters to foreign jurisdictions on behalf of the Australian law enforcement authorities, including the Australian Crime Commission.
- Coordinating the provision of assistance from other countries for the investigation and prosecution of crime and the restraint and confiscation of assets of crime.

2.48 In addition, the submission advised that Australia is party to a number of bilateral Mutual Assistance in Criminal Matters treaties. Assistance can be provided to countries with which Australia does not have formal treaties, through the *Mutual Assistance in Criminal Matters Act 1987*. This legislation enables Australia to provide assistance on request in relation to taking of evidence, issuing of search warrants, forfeiture, confiscation, or restraining of dealings in property associated with criminal offences, and the recovery of penalties.

2.49 Section 8 of the *Mutual Assistance in Criminal Matters Act 1987* specifically provides that the Attorney General must refuse the requested assistance in cases where the death penalty may be imposed, unless the Attorney is persuaded that special circumstances exist. Cases in which the request may be refused include political prosecutions, and the prosecution of a person for an act or omission that if it had occurred in Australia, would have been an offence under the military law of Australia but not also under the ordinary criminal law of Australia.

2.50 There are several international treaties which affect Cybercrime, including the UN Convention on Transnational Organised Crime, which focuses on international co-operation against crimes such as money laundering. In addition the Council of Europe and the Lyon Group have established networks of law enforcement officers which are operated by Interpol. The AFP is the contact point with this network.[22]

2.51 The Committee also notes that limitations in Australia's domestic legislation prevents assistance being provided to other countries in cases in which telecommunications intercept and listening device material is requested.

2.52 The *Telecommunications (Interception) Act 1979* does not allow Australia to gather intercept and listening device material on behalf of another country. The exception is where the material has already been obtained for an investigation of an Australian offence.[23]

2.53 There are also least 13 Commonwealth Acts of Parliament which have some regulatory relevance to cybercrime (see Appendix 5). In addition, states and territories have their own legislation which is not uniform, either in offence provision or in penalties. The ACC submission gives the example of a lack of uniformity in

22 Submission no.21, pp 7-8

23 Submission no.21, p.15

Commonwealth and State laws as they apply to Internet Content Hosts (ICH)[24] and Internet Service Providers (ISPs). Commonwealth law applies to ICHs but not to content providers, creators or ordinary Internet users. State legislation applies to content providers and ordinary Internet users.[25]

2.54 The state governments focus on the offences which, while they can be committed by electronic means, are 'traditional' criminal offences – for example – fraud, or possession of child pornography. The means to these offences is via a telephone connection, and this is an area of Commonwealth responsibility.

2.55 The Committee notes that there are at least two bodies which could address this lack of consistency, and promote a more focussed and unified approach to the investigation, detection and prosecution of cybercrime. They are: the Standing Committee of Attorneys General, and the Police Ministers' Council.

2.56 The Committee is concerned that while there is no common cybercrime regime in Australia, there is an increasing likelihood of this weakness being exploited by criminal elements.

Internet Service Providers (ISPs) and Internet Content Hosts

ISP's

2.57 Internet Service Providers sell Internet access. The Internet Industry Association website explains the process of providing Internet access. In short, clients require a modem (computer access to a telephone system) and usually enter a contract to pay a monthly fee to use the service. This is usually paid by credit card. The ISP provides software, and a telephone number to provide the Internet access. The client selects a user name and password – which identify him or her to the ISP when access to the Internet is required. The client can then use the World Wide Web, and send and receive email. In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company's networks to the Internet. ISPs themselves are connected to one another through Network Access Points (NAPs). ISPs are also called IAPs (Internet Access Providers).[26]

2.58 ISP's are not licensed. Anyone (with appropriate information technology skills) can establish themselves as a provider. In this unregulated environment, a number of concerns have emerged.

---

24 The Internet Industry website at http://www.iia.net.au defines Internet Content Hosts as persons who host Internet content in Australia or who propose to do so (this is a similar definition to that in Schedule 5 of the *Broadcasting Services Act 1992*. Examples include a webfarm such as webcentral or a person who has their own website or server and hosts content provided by a range of contributors.

25 Submission no. 23, p.53

26 www.iia.net.au

2.59 The resources of less reputable ISPs can become a storehouse for records of criminal activity. Further there is potential for ISP's to obtain material from client addresses which is confidential, in addition to the credit card payment information which is supplied by the clients when they join the service.

2.60 ISP's are not nationally limited. They can operate from Australia to anywhere in the world, as can international operators operate in Australia. There would be a significant expense for small providers to do this, but it is possible.

2.61 There have been some initiatives in other jurisdictions to minimise the criminal potential associated with ISPs. In evidence Mr. Greg Melick told the Committee that the United Kingdom has legislation which specifies that acts or results occurring in the UK are subject to UK jurisdiction. He continued:

> … until we start enacting appropriate laws, both as to jurisdiction and preservation of evidence, we are not going to get very far.[27]

Internet Content Hosts

2.62 The expression Internet Content Host (ICH) is one which appears to be used in Australia, and few other places. It is defined in Clause 3 of Schedule 5 of the *Broadcasting Services Act 1992* as:

> … A person who hosts Internet content in Australia, or who proposes to host Internet content in Australia.

The Schedule also states that Internet content means information that:

> (a) is kept on a data storage device; and
>
> (b) is accessed, or available for access, using an Internet carriage service;
>
> but does not include:
>
> (c) ordinary electronic mail; or
>
> (d) information that is transmitted in the form of a broadcasting service.

2.63 An Internet Service Provider can also host Internet content, and in practice many do so. These are services which organise and design materials for persons who wish to provide information on the Internet.

2.64 Invitations were extended to Internet Service Providers, and the Internet Industry Association to provide the Committee with a submission to give the Committee an opportunity to hear first-hand what the issues are which are most significant for the service providers and the industry as a whole. None was forthcoming. The Internet Industry Association did provide the Committee with a

---

27 *Committee Hansard* ,21 July 2003, p. 28

copy of the draft code of conduct which is discussed below. However, the Committee had no opportunity to discuss the Code of Conduct or to address associated issues to the industry peak body and industry participants.

Co-operative schemes, and codes of conduct

2.65 The Committee heard that there are international, interdepartmental, Federal/ State government and private sector committees examining the issue of Internet regulation. The Attorney General's Department submission lists no fewer than nine 'cybercrime stakeholders',[28] each of which is working on its own projects involving cybercrime. The submission notes that the Australian Securities and Investments Commission (ASIC) has been working with the Internet Industry Association on a Cybercrime Code of Practice. The association has a wide ranging membership which includes telecommunications carriers, ISPs, e-commerce solution architects, hardware and software vendors and content providers.

The Internet Industry Code of Practice

2.66 The Internet Industry Code of Practice was released by the Internet Industry Association on 21 July 2003, and was provided to the Committee on 8 September 2003. Through self regulation, the Code aims to establish a co-operative working environment between law enforcement agencies (LEAs) and the Internet Industry Association. The code aims to:

- Establish clear guidelines for criminal and civil investigations within the provisions of the *Telecommunications Act 1997* (the Act).
- Establish clear guidelines (within standards of confidentiality and privacy established under the Act) agreed between industry and LEAs as to what constitutes 'such help as is reasonably necessary'. This also is intended to establish public confidence in, and promote the use of the Internet.
- Provide a transparent mechanism for the handling of LEA's investigations for the Internet industry which is clearly understood by both parties.
- Promote positive relations between the LEAs and the Internet industry.
- Give users of the Internet confidence that their privacy and the confidentiality of their transactions will be guarded from unlawful intrusion by LEAs.[29]

2.67 The Committee is concerned about the persuasive effect of the Code. If the Code of Conduct applies only to those who agree to be bound by it, there is still a potential for the problems which the Committee's terms of reference identifies to remain unsolved, as those who wish to operate free of sanctions will still be able to do so.

---

28 Submission no. 21, pp 19-23

29 Internet Industry Code of Practice, paragraph 1.11.

2.68 The Committee considers that the matter of regulation of ISPs should be examined more closely, not only in the context of ensuring the compliance of ISPs with a set of standards, but also in the context of the jurisdictional and evidentiary issues which have emerged in the Internet environment, and which rely on the material held by ISPs.

Recommendation 1

The Committee recommends that the House of Representatives Committee on Communications, Information Technology and the Arts examine the regulation of Internet Service Providers, including codifying the jurisdictional and evidentiary matters involving material which is transmitted or held by the Provider.

2.69 The Committee considers that there is a very strong case for a central co-ordinating body for Cybercrime offences, and a form of regulation which applies to those who refrain from endorsing the Code of Conduct.

Detecting and prosecuting cybercrime

2.70 During the inquiry the Committee became aware of a number of issues that apply generally to the detection of cybercrime and the collection of evidence for prosecution. With anonymising software (which can redirect and divert material), and the ease with which free email addresses can be obtained without supporting identification, detection of cybercrime is difficult and resource intensive.

2.71 The NSW Police also told the Inquiry that it is possible to compromise the actual domain server, 'thereby being able to re-route traffic, say from an Internet banking site.[30] While the Police said this had not actually occurred, the Committee considers it is a possibility which any protective strategy must bear in mind.

2.72 Other methods of masking illegal Internet activity include cryptography and steganography. The former involves encrypting of data so that it is unintelligible; steganography allows illegal data to be contained in seemingly innocuous files, such as photographs, which can then be reworked at its destination so as to allow access to the illegal data.

2.73 One important issue drawn to the Committee's attention was the gathering of evidence in the cybercrime environment. The Committee observed that the in the cyber environment the evidence trail disappears rapidly. There are devices which allow material to be 'scrubbed' from a storage medium; further, as ISPs are not required to retain records, there can be little material left to investigate.

2.74 While it is possible to obtain search warrants to seize computer hard drives, discs and other records, there appears to be no legal way in which Internet activity can

30 *Committee Hansard,* 18 July 2003, p.83

be monitored in 'real time' as can be done with an authorised telephone intercept device, obtained under the *Telecommunications (Interception) Act 1979* (Cth).

2.75 The ACC suggested in its submission[31] that the powers available under section 25A of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) might also be made available to the ACC in cybercrime investigations (although in giving evidence in Sydney the ACC clarified this and indicated that this was one possibility among many for the future).[32] These powers would allow real time surveillance of computer based activity to search computer data for a period up to 6 months. The ACC proposed that this – as with the ASIO legislation – would be subject to the issuing Minister being satisfied on reasonable grounds that the intelligence collection will be substantially assisted by the content which is obtained under the warrant.

2.76 The ACC did not press this, and explained that:

> … we are just scoping into the future of electronic policing requirements maybe five or 10 years away. We are not saying that the ACC should have these powers; we are just saying that this is another law enforcement tool that in the future may be directly related to electronic crime investigation.[33]

2.77 The powers suggested effectively offer a licence to hack into other computers. The ACC presented the argument that:

> Such a monitoring warrant enables law enforcement to use investigative tools … to intercept and collect the communications of the subject of the warrant while ignoring those communications which the authorisation to intercept does not cover.
>
> Analogous to telephone intercept warrants in all material respects computer monitoring warrants, issued subject to the same administrative and judicial requirements and safeguards as telephone intercept warrants – would significantly enhance the investigative tool kit available to law enforcement.[34]

2.78 The Committee notes that the provisions of section 25A of the ASIO Act are very limited in their application: they apply only to instances where national security is threatened. There was some discussion during the hearings as to whether powers such as this were appropriate in this context, or whether they should be limited to the provisions of the ASIO Act.

2.79 The practicalities and likely benefits were canvassed in evidence by Mr Gregory Melick, who told the Inquiry:

---

31 Submission no.23, p.55

32 *Committee Hansard*, 18 July 2003, p.5

33 *Committee Hansard,* 18 July 2003, p.5

34 Submission no 23, pp.55-56

> Most of your relevant data and evidence for law enforcement purposes will come from computer hard drives. Once you get that information, you then should be able to go to the various Internet providers to get the preserved data to get your evidentiary trail to lead you to the perpetrator … To randomly try to pluck something out of the ether and interpret it to see what is going on will be almost impossible. You also have the other problems of encryption and steganography.[35]

2.80 The proposed warrants were for telecommunications devices. However, as was pointed out to the Committee, wireless technology, which is not covered by the telecommunications legislation, is being used increasingly in communications.[36] In his submission Mr. Steve Orlowski said

> … failure to develop secure wireless products and applications could raise public concerns over wireless security and slow the spread of this potentially valuable new technology. Economic progress and the strengthening of cyber-security require addressing these concerns.

2.81 Accordingly, any regulating of the Internet environment must account for those who will use wireless technology as well as telecommunications.[37]

2.82 The Committee notes that the need for continuous legislative review, in the light of operational information is fundamental to the detection and prosecution of cybercrime.

Privacy

2.83 The Committee noted that there was some concern regarding privacy and the collection of evidence. In their submission to the Inquiry, Electronic Frontiers said:

> We are concerned … by the increasing prevalence of legislative proposals and laws concerning the Internet that fail to contain an appropriate balance between individuals' privacy and the legitimate needs of law enforcement agencies.[38]

2.84 In evidence to the hearing, the AHTCC indicated that it is aware of the need to balance the right of individuals to privacy of communications and the right of individuals to be protected against criminal activities.[39] A similar sentiment was expressed by ASIC which has been involved with other agencies in advising the

---

35 *Committee Hansard,* 21 July 2003, p.32

36 *Committee Hansard*, 17 July 2003, p.13

37 Mr Steve Orlowski, Submission no 9, p.17

38 Submission no 4, p.3

39 *Committee Hansard*, 21 July 2003, pp.19-20

Internet Industry Association on its proposals for a code of practice which seeks also to address the privacy issue. [40]

2.85 The Committee noted that there is an overall tension between the preservation of privacy and protection of children from unsuitable content and consumers generally from unwanted emails and from malicious material such as viruses.

Technological development

2.86 It has become clear to the Committee that crime authorities must be able to keep pace with the advance of technology. The latest (at the time of writing) 'g3 technology' which allows the mobile telephone to become a portable multi media device will require a reconsideration of the differentiated approaches to the regulation of single function devices.

2.87 The Committee observed that organised crime is well able to fund its own development in this area, for obvious reasons. Further, advances in communications technology enhance the ability of criminal groups to organise themselves at an international level.

2.88 Law enforcement will usually be in a reactive rather than an active position, but the Committee considers that with the right strategic development, agencies will be well placed to at least meet, if not anticipate the increasing challenges of rapid technological development. There appears to be a considerable amount of work being undertaken: there is legislation being prepared by the Attorney General's Department, numerous Committees and interagency discussions, but the Committee considers that this activity needs a well resourced co-ordinating body. The following chapters detail examples which illustrate this more clearly.

40 *Committee Hansard,* 21 July 2003, p. 39