Australian Government Response to the Recommendations of the Parliamentary Joint Committee inquiry on Cybercrime

Australian Government Response to the Recommendations of the Parliamentary Joint Committee inquiry on Cybercrime

Chapter 2 - Crime in Cyberspace

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.

Accept

The Government supports an examination of this issue by the House of Representatives Committee on Communications, Information Technology and the Arts.

Chapter 3 - Cybercrime and Internet paedophile activity

Recommendation 2
The Committee recommends that the Government investigate partnerships for establishing a multimedia public education campaign on the risks associated with and the safe use of information technology by children, including parental supervision.

Accept

The Government notes the Committee's support of the Australian Broadcasting Authority's (ABA) community education role in the context of the Online Content Scheme and would like to bring to the Committee's attention the role and activities of NetAlert. The Government considers that the activities of NetAlert address the Committee's recommendation concerning the establishment of a multimedia public education campaign on the risks associated with the safe use of information technology by children, including parental supervision.

The Government established NetAlert under the Online Content Scheme in December 1999 as an independent body to promote Internet safety, particularly for children, and to provide the community with sensible, helpful and reliable advice about family-safe use of the Internet. In addition to undertaking community education, advice and research activities, NetAlert functions as the designated statutory body for the purposes of the Online Content Scheme, requiring it to be consulted during the development of Internet industry codes and standards prior to registration by the ABA.

In the last three years NetAlert has undertaken a national multimedia campaign on a range of Internet safety issues, involving the establishment of an advisory website for parents, teachers and industry bodies and an interactive children's website. NetAlert has distributed a range of materials containing Internet safety advice and information, including posters and brochures and has promoted its services through the broadcast of national radio and television community service announcements. NetAlert has developed

and implemented the first phase of its *CyberSafe Schools Project*, a three-year initiative to educate school students across Australia about the safe and responsible use of the Internet.

In addition to these initiatives, NetAlert continues to operate its toll free Internet safety helpline and email advisory service.

NetAlert has established a number of strategic alliances or partnerships with key Internet industry bodies, including the Internet Industry Association, Internet Society of Australia, the Australian Telecommunications Users Group and the Service Providers Action Network.

As part of the Government's *National Child Protection Initiative* election commitment, NetAlert will receive funding of $2 million to run a National CyberSafe Program (NCP) which will deliver a two-year targeted training roadshow and information campaign aimed at educating parents, teachers and community groups about online safety.

The funding to be provided to NetAlert for the NCP complements other funding being provided under the initiative to the Australian Federal Police (AFP). The AFP will receive funding of $1.7 million for the continuation of its important education and prevention programs aimed at parents, teachers and relevant community groups. On 1 January 2005 the AFP received a total of $28.4 million over three and a half years under the *National Child Protection Initiative* to set up a national centre for major international and national referrals of child sex abuse material and images with the power and resources to target, infiltrate and shut-down organised online paedophile networks.

Recommendation 3
The Committee recommends that the Commonwealth Attorney-General liaises with the State and Territory Attorneys-General to ensure that priority is given to the development and implementation of consistent offence and evidence legislation in relation to cybercrime, which is in accordance with Australia's international obligations.

Accept

The Government has been very proactive in combating new and emerging technological developments in crime and has already taken steps to ensure implementation of nationally consistent legislation on cybercrime.

Computer offences

The *Cybercrime Act 2001* came into force on 21 December 2001. The Act added Part 10.7, which contains computer offences, to the *Criminal Code*. These computer offences are based on the January 2001 Model Criminal Code Officers' Committee (MCCOC) Report on *Damage and Computer Offences* developed in cooperation with the States and Territories through the Standing Committee of Attorneys-General and are consistent with the Council of Europe Convention on Cybercrime.

To date, five State and Territory jurisdictions (South Australia, New South Wales, Victoria, the Australian Capital Territory and the Northern Territory) have implemented

the model computer offences in the MCCOC Report. The Government has repeatedly emphasised to States and Territories at Standing Committee of Attorneys-General meetings the importance of fulfilling their commitment to a national model criminal code by promptly implementing the proposals in MCCOC reports.

Part 10.7 of the *Criminal Code* provides that those who engage in the unauthorised use of a computer with the intention of committing a serious offence such as fraud are subject to the maximum penalty which applies to the serious offence they intend to commit. Part 10.7 also includes an unauthorised impairment of electronic communications offence which targets disruptive tactics such as 'denial of service attacks' with a maximum penalty of 10 years imprisonment. Similarly, an offence of unauthorised modification of data to cause impairment to that data or any other data attracts a maximum penalty of 10 years imprisonment.

Part 10.7 of the *Criminal Code* also contains offences directed at those who possess or trade in programs and technology designed to damage data in other people's computer systems. The offences of possessing or supplying data with intent to commit a computer offence are subject to a maximum penalty of three years imprisonment.

Other offences include unauthorised access to or modification of restricted data and unauthorised impairment of data held on a computer disk or other device; both of these offences attract a maximum penalty of two years imprisonment.

The *Cybercrime Act 2001* also updated federal investigation powers in the *Crimes Act 1914* and the *Customs Act 1901* to ensure they cater for the new electronic environment. Law enforcement officers executing a search warrant are able to search not only material on computers located on the search premises but also material accessible from those computers but located elsewhere. Officers also have enhanced powers to copy data and to move computer equipment and disks off the search premises.

In addition, law enforcement officers can apply to a magistrate for an assistance order, requiring a person with knowledge of a particular computer system to provide the officer with the assistance necessary to enable the officer to access, copy or convert data on the computer system.

Credit and debit card skimming and Internet banking fraud

The Committee's report highlights the growing incidence of credit and debit card skimming and Internet banking fraud. The Government has also taken steps to develop a nationally consistent legislative response to these issues.

In March 2004, the Standing Committee of Attorneys-General released the Model Criminal Code Officers' Committee Discussion Paper on Credit Card Skimming Offences. The discussion paper identified a gap in federal, State and Territory laws in their coverage of credit and debit card skimming and included a model offence to address this gap. The model offence criminalises dishonestly obtaining or dealing in personal financial information without the consent of the person to whom the information relates. The model offence is drafted in technologically neutral terms to ensure that it will not be overtaken by developments in the techniques or equipment used to capture credit or debit card data or other personal financial information (such as a person's username and password for Internet banking).

The Government has quickly implemented the model offence, together with offences which target the possession and importation of devices used to 'skim' data from credit and debit cards. These offences are included in the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No.2) 2004* which commenced on 28 September 2004.

Recommendation 4
The Committee recommends that as part of its legislative package to detect and prosecute those who use information technology for the trade of child pornography, the Government introduce a new offence relating to luring and grooming children for sexual purposes.

Accept

The Government takes its responsibilities to safeguard Australia's children from sexual predators very seriously and has already criminalised the practice known as 'online grooming'. On 14 March 2004, the then Minister for Communications, Information and the Arts, the Hon Daryl Williams AM QC MP, and the Minister for Justice and Customs, Senator the Hon Chris Ellison, released an exposure draft of the legislative package mentioned in the Committee's recommendation for public comment.

Following public consultation, the Government enacted the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No.2) 2004*. This Act provides for 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 'grooming' offences prescribe maximum penalties of imprisonment for 12 years. The 'procuring' offences impose maximum penalties of imprisonment of 15 years. The offence regime operates nationwide in the same way that the other telecommunications offences targeting persons who access, transmit or make available child pornography or child abuse material.

The offences target both these steps. Relevant legislation in Queensland and the United Kingdom was considered in developing the offence regime. Where appropriate the proposed offences are consistent with the existing federal child sex tourism offences in Part IIIA of the *Crimes Act 1914*.

Recommendation 5
The Committee recommends that the Australian Crime Commission in conjunction with the Australian High Tech Crime Centre investigate the provision of general information on fraud trends to financial institutions through a secure subscription based service.

Accept

The Government supports the recommendation. The Australian High Tech Crime Centre (AHTCC) and the Australian Crime Commission (ACC) are working together in addressing high tech crimes against banking and financial institutions.

On 20 May 2004 the Commonwealth Minister for Justice and Customs, along with the Commissioner of the Australian Federal Police and representatives of the banking and finance sector, launched the Joint Banking and Finance Sector Investigations Team (JBFSIT). The JBFSIT is supported by the Australian Bankers' Association as well as the Credit Union Services Corporation (Australia) Limited, Visa International and MasterCard International. The JBFSIT has seconded specialised personnel from Australia's five largest retail banks attached to the AHTCC. In addition, the JBFSIT works closely with the Australian Computer Emergency Response Team (AusCERT) on technical analysis matters.

The JBFSIT produces intelligence and operations assessments for consumption of the banking and finance sector identifying trends and vulnerabilities.

The ACC has also implemented strategies that address this recommendation which included the part time secondment of an intelligence analyst to the AHTCC in February 2005 for a period of six months. Through the Australian Law Enforcement Intelligence Net (ALEIN) and the Australian Criminal Intelligence Database (ACID) the ACC has in place a mechanism for the efficient and effective sharing of information/intelligence with the Australian law enforcement community. Of particular note is the ACC's maintenance of a 'National Fraud Desk' which operates with funding arrangements under the Inter-Governmental Agreement (IGA). One of the new joint-initiatives of the ACC and the AHTCC is the proposed development of a new information and intelligence desk for ALEIN on high tech crime. Subject to security and privacy requirements, and consistent with the dissemination powers of the ACC, information held in ALEIN desks is communicated to financial institutions through mechanisms such as the Fraud Desk 'fortnightly digest'.

Recommendation 6
The Committee recommends that the Australian Crime Commission, in consultation with the Australian High Tech Crime Centre, AUSTRAC and other law enforcement agencies give priority to developing a national intelligence gathering strategy for cybercrime in the banking industry. Further the ACC should seek to fill any gaps in intelligence holdings that are identified.

Accept

The Government believes that the activities outlined in recommendation 5 will address gaps in intelligence gathering strategies for cybercrime in the banking industry.

In addition to meeting its statutory responsibility through the provision of the services offered by ALEIN/ACID (see response to recommendation 5 above), the ACC has recently commenced an intelligence scoping project that examines a wide range of fraud issues affecting the financial sector, including consideration of the role of cybercrime. The Major Fraud probe is identifying a range of fraud related issues that have/are emerging in the high-tech area. This will culminate in the development of a Strategic Criminal Intelligence Assessment which identified key threats to Australian law enforcement. The ACC's role in developing National Criminal Intelligence Priorities for consideration by the ACC Board provides opportunities to identify intelligence gaps and to seek to address them in collaboration with a range of partners through the ACC-managed 'National Criminal Intelligence Collection Requirements'.

Chapter 6 Further developments and conclusion

Recommendation 7
The Committee recommends that the Government include in its cybercrime strategy, directed training for law enforcement agencies, and the development of a whole of government approach in which individuals can gain expertise which can be shared between those agencies.

Accept

The Government recognises that there is a need for specialised and continuous training for practitioners in this field, both in terms of the underlying technical theory and in the use of vendor-specific applications. This training must be ongoing to cope with the changing nature of high tech crime.

The AHTCC is responsible for implementing the Australian E-Crime Strategy, which has as one of its core features joint training and interoperability of specialised high tech crime and computer forensic units. As part of its commitment to this objective, the AHTCC hosted the second annual AHTCC/AFP Forensic Computing and Computer Investigations Workshop in March 2005 to provide specialist training courses for high tech crime practitioners across all Australian state police forces, Commonwealth revenue, regulatory and enforcement agencies and selected private sector organisations with an interest in this type of matter. The workshop participants examined and discussed critical issues that arise in responding to incidents related to computer investigations and contemporary computer forensic practice, including innovative tools, latest software updates and gaps.

The AHTCC is examining a range of training options to improve the skill of Australian Police services.

Establishment of the proposed joint ALEIN site will provide an excellent conduit for the sharing of intelligence and information that could be diverted to the training area.

Over the last three years, the ACC Cyber Support Unit has provided Cybercrime Investigations Training to some 176 ACC, Seconded Police and partner agency staff. In addition, there are 52 personnel currently undertaking this training. This training of Seconded Police and Partner Agency staff provides the jurisdictions with a core expertise in this area. The Cyber Support Unit has also assisted a number of partner agencies in development of their own in-house Cybercrime Investigations courses.

The ACC Cyber Support Unit also continues to promote the establishment of National Computer Forensic "Digital Evidence Groups" (DEG), which focus on Law Enforcement Cybercrime technical expertise. ACC members currently chair the DEG groups from NSW and Victoria, and the ACC recently promoted the concept with Regional Law Enforcement Agencies in Hong Kong.

Recommendation 8
The Committee recommends that the Australian Crime Commission continue its current level of involvement in Cybercrime investigation, and intelligence gathering, as well as further developing its international liaison role.

Accept in part

The Government notes that the AHTCC is the agreed national body for high-tech crime matters and as such is the primary conduit for investigative operations and, through the AFP, international liaison activities. The AHTCC has seconded officers from each Australian jurisdiction and is the national centre for high-tech crime and the holder of the national e-security agenda. It is the body best placed to lead the investigative response to most instances of high tech crime which impact on Australia.

The ACC complements this role by providing a national criminal intelligence collection and analysis capability augmented by a Cybercrime investigative capacity to support its investigative capabilities.

The Government notes that the ACC will continue to encounter Cybercrime during the course of its work and will continue to work closely with the AHTCC as appropriate in fully investigating activity encountered.

The Government notes that the AFP will continue existing arrangements which provide international liaison services to the ACC via its international police liaison officer network.

In conjunction with the AFP international liaison officer network, the AHTCC has (with AFP support) been strengthening bilateral links with entities such as the United Kingdom's National High Tech Crime Unit, the United States Secret Service and the

Royal Canadian Mounted Police. The ACC benefits from these links via its close working relationship with the AFP and AHTCC.

The Government also notes that the AHTCC is the national contact point for a range of international initiatives, including the Council of Europe G8 24/7 contact list for the preservation of IT evidence and the Virtual Global Taskforce – an international alliance of law enforcement agencies to make the internet a safer place.

Recommendation 9
The Committee recommends that the Australian Crime Commission ensure its information sharing strategies, including liaison with the Australian High Tech Crime Centre, maximise the opportunities for giving and receiving accurate and timely information about cybercrime methods and technology.

Refer to Recommendation 8

Recommendation 10
The Committee recommends that the Australian Crime Commission seek out opportunities to participate in appropriate public/private sector cybercrime projects, to promote the sharing of information, and the efficient prevention and investigation of cybercrime offences.

Accept

The Government notes that the commitment of a part-time intelligence analyst from the ACC to the AHTCC reflects the level of the ACC's support for its work with the AHTCC and through that secondment arrangement the ACC has access to a wide range of public and private sector interests focusing on dealing with cybercrime. The ACC's current and projected work on fraud (notably identity fraud) matters includes joint projects with the private sector as well as with government and regulatory agencies.

The ACC's Cyber Support Unit has established private sector partnerships including forensic training from Apple Computers, liaison with the credit card companies in regards to trends and card skimmer forensics. It also offers assistance to partner agencies and is forming technical partnerships with overseas law enforcement agencies in internet intelligence gathering.

The AHTCC's JBFSIT and other public private partnerships with industry sector organisations is providing leading edge training and direct access to industry knowledge and expertise on cybercrime and related matters. The AHTCC is the best placed body to represent law enforcement in a national approach to public private partnerships for high tech crime matters.

The ACC also financially contributes to the development of the National AUSCERT Alerts Reporting Scheme, with other partners. This alert scheme are a public/private sector initiative, aimed at providing a national response to cybercrime incidents.

Recommendation 11
The Committee recommends that the Australian High Tech Crime Centre act as a clearing house for information on cybercrime, in order to explore initiatives to combat it.

Accept

The Government notes that the ACC is assisting the AHTCC to develop a secure national cybercrime referral system within ALEIN.

In addition, the AHTCC and state and territory jurisdictions have also agreed to use the ACC ACID system as the primary intelligence recording tool for cybercrime matters.

The AHTCC not only receives and disseminates criminal intelligence both nationally and internationally, it also takes a lead role in coordinating relevant investigations within Australian and international jurisdictions. The AHTCC is best placed to continue this important role.