



**Crimes Legislation Amendment
(Serious and Organised Crime) Bill
(No. 2) 2009**

**Submission by the
Australian Federal Police (AFP)**

October 2009

Introduction

The Australian Federal Police welcomes the opportunity to make a submission to the Senate inquiry into the *Crimes Legislation Amendment (Serious and Organised Crime) Bill (No. 2) 2009*. The Bill introduces the second phase of the Commonwealth legislative amendments targeting serious and organised crime. The AFP supports the measures contained in the Bill that will enhance AFP operational capacity to investigate and prosecute organised criminal activity.

This submission is structured in five parts focussing on the key schedules contained in the Bill that will enhance AFP operational capability.

- A. Schedule 1 – Proceeds of crime
- B. Schedule 2 – Search warrants
- C. Schedule 3 – National Witness Protection Program
- D. Schedule 4 – Criminal organisation and association offences
- E. Schedule 5 – Money laundering
- F. Schedule 9 – Drug importation

A. Proceeds of Crime

Amendments to the definition of “effective control”

The AFP support the amendments to the definition of “effective control” which make it clear that this term covers property that is under the control of more than one person.

Problems with the definition of effective control were highlighted during Project Wickenby when a restraining order was sought over monies held in a joint bank account.

In April 2008, Commonwealth agency investigations under Project Wickenby identified monies held in a series of jointly held bank accounts as being unlawfully obtained.

The AFP sought to restrain the funds in the jointly held accounts under the Proceeds of Crime Act provisions.

However, prosecuting authorities advised that the notion of “effective control” was narrow, and could require that the suspect individual had sole control over the operation of the bank account before a restraining order could be issued.

Whilst the issue was being resolved, ten million dollars was moved out of the accounts and out of the Commonwealth’s reach.

The New South Wales Crime Commission agreed to seek to restrain the balance of the accounts under s 10A of the NSW *Criminal Asset Recovery*

Act 1990. The relevant provisions in the *Criminal Asset Recovery Act 1990* are broader than those in the Commonwealth Act.

Amendments to the definition of “account”

The AFP support the amendments to the definition of “account” expanding this term to encompass credit card accounts, loan accounts, accounts held in the form of units such as a cash management trust and closed accounts.

As the Sherman Report observed, all types of accounts are potential safe harbours for proceeds of crime and they become particularly attractive to criminals if they are beyond the reach of investigative powers provided under the Act.

Closed accounts can also prove to be valuable sources of information. As the legislation currently stands, individuals are able to prevent information relating to transactions involving proceeds of crime being obtained simply by closing their accounts.

This amendment will expand the reach of section 213 notices to financial institutions to require institutions to provide information relating to all types of accounts including those run outside the mainstream financial institution framework.

Obtaining details of stored value cards from Financial Institutions

Stored value cards refer to cards which have credit loaded onto the card itself which can then be used at places which honour the card. Loyalty cards and gift cards are examples of stored value cards designed to replace cash transactions. A stored value card is essentially cash in another form. As such these cards have a very high money laundering vulnerability.

Stored value cards have been known to be used to launder money from the proceeds of narcotics and pay drug couriers.

These cards operate extensively in some overseas countries where they are primarily used as transit cards (Hong Kong and Singapore for example), but they can also be used to purchase low value goods and/or meals from establishments that accept the cards.

Information gathering powers such as monitoring powers and notices to financial institutions are currently only exercisable with respect to “accounts” held by financial institutions.

Because stored value cards are not generally linked to an account there is currently no way to obtain information on transactions made using these types of cards.

Amendments introducing references to “stored value cards” will enable the AFP to direct information-gathering powers such as monitoring powers

and notices to financial institutions to capture details of transactions using these cards.

Amend s 225 to Search warrant

The AFP support the amendments which will extend s 225 search warrants to enable them to cover property that is proceeds of a foreign indictable offence or evidence relating to benefits derived from the commission of such an offence.

This amendment fixes a gap in that the *Proceeds of Crime Act 2002* provides mechanisms to undertake proceeds action in relation to foreign indictable offences, however the current search warrant provisions do not allow the AFP to obtain a search warrant enabling searches of premises where there are reasonable grounds to suspect that tainted property or evidential material relating to foreign indictable offences is present.

The current limitations on s 225 search warrants could also potentially frustrate mutual assistance requests from Australia's international partners by preventing search warrants being carried out to investigate the proceeds of foreign offences transferred to Australia.

B. Search warrants

Law enforcement agencies have become increasingly reliant upon electronic equipment as a source of evidential material to assist in the investigation and prosecution of criminal activities. Advances in technology have resulted in the emergence of increasingly complex electronic equipment that has the capacity to store large volumes of data. Such equipment is readily accessible and affordable; accordingly there is a necessity for law enforcement agencies to build on their capacity to examine such equipment. Effective legislative provisions that provide mechanisms to access and search electronic equipment are essential to enable law enforcement agencies to combat criminal activity efficiently.

Division 2 of Part 1AA of the *Crimes Act 1914* contains provisions that relate specifically to search warrants, including when a search warrant can be issued, things that are authorised by a search warrant, assistance that may be sought to execute a warrant and the use of equipment to examine and process things at the warrant premises.

The existing search warrant provisions pertaining to the examination of computers on warrant premises were introduced in the *Crimes (Search Warrants and Powers of Arrest) Amendment Act 1994* when personal computers were not as widely used as they currently are. Furthermore, computers were more expensive, cumbersome and potentially fragile if moved. Tests that were imposed for police to examine computers on warrant premises were designed to ensure that electronic equipment was only operated to establish whether it contained evidential material where the officer believed the equipment could be operated without causing

damage. Today electronic equipment is quite readily able to be accessed, copied and moved by police (with assistance from computer specialists where necessary) with negligible risk of any damage to the equipment.

As a consequence of further advances in technology, particularly the exponential increase in the storage capacity of computers, a number of limitations have been identified with the existing search warrant provisions in Part 1AA, specifically those relating to electronic equipment.

The proposed amendments contained in Schedule 2 of the Bill that relate primarily to the use, sharing and retention of seized material and the examination and processing of electronic equipment for evidential material will alleviate these deficiencies.

Operation of electronic equipment at warrant premises

The AFP supports amendments to provisions governing the use of electronic equipment at warrant premises. These include:

- Removal of the existing requirement for executing officers to believe on reasonable grounds that data on electronic equipment on warrant premises might constitute evidential material before operating the equipment; and
- Lowering the threshold for police to copy and take away data accessed by operating the equipment at the warrant premises to where the executing officer or constable assisting "suspects" on reasonable grounds the thing contains of constitutes evidential material.

Currently section 3L(1) places a requirement upon police executing a search warrant to believe on reasonable grounds that data on the electronic equipment on the warrant premises might constitute evidential material before operating the equipment. This test is at odds with the section 3F search warrant authority for executing officers to examine everything within the warrant premises, including electronic equipment. Data stored electronically is indistinguishable from documents containing data stored in a filing cabinet in the warrant premises. The repeal of section 3L(1) will overcome this conceptual issue by enabling executing officers to search electronic equipment like any other item located on warrant premises for evidential material under the authority of the warrant alone. It will also overcome existing operational difficulties in establishing the requisite "belief" that electronic equipment may contain evidential material without an examination of equipment in circumstances where there is no other supporting evidence.

The AFP support reducing the threshold for police to copy and take away some or all data accessed by operating equipment at warrant premises. During the execution of a search warrant it may not be practicable to search all electronic equipment owing to the volume and complexities of the computer system and time restrictions. For this reason, the capacity to copy and take data away from the premises after a preliminary

examination is an important mechanism necessary for police to conduct their investigations efficiently. Copying data will avoid the disruption that the seizure of a computer can cause to a person or business and mitigate any potential loss that may be suffered by an occupier.

For example, where a search warrant is executed upon a business and a preliminary examination of electronic equipment used to run the day to day operations of the business reveals some evidential material, the new provisions will enable police to copy some or all of the equipment and conduct a more comprehensive analysis of the data away from the warrant premises. Scope to copy and take data away after a preliminary examination will reduce the time that police will need to remain at the warrant premises examining the equipment thereby reducing disruption to the business caused by police presence. More importantly, taking a copy for further examination as opposed to seizing electronic equipment will ensure that the business is able to continue trading as normal after the execution of the search warrant whilst police continue examining the remainder of the data for further evidential material using the copy taken during the execution of the search warrant.

Operations of electronic equipment at another location

With the growing complexity of electronic evidence, operationally it is not always possible to effectively search electronic equipment at search warrant premises. In some circumstances encryption will prevent police from conducting any search of the equipment.

The AFP support amendments contained in the Bill that will enhance the capacity for police to examine equipment at another location. Key amendments include:

- Reducing the threshold for moving a thing to another place for examination where the constable “suspects” on reasonable grounds the thing contains or constitutes evidential material;
- Extending the timeframe for examination and processing of equipment from 72 hours to 14 days with an option(s) to extend the time for a further 7 days;
- Allowing an exception to compliance with the obligations to inform the occupier of the location where the seized equipment will be examined and to allow the occupier to be present during the examination where the executing officer believes on reasonable grounds compliance may endanger the safety of a person or prejudice the investigation or prosecution; and
- Inclusion of an authority for police to copy things off-site, so that the original item can be returned to the owner.

Moving equipment for examination

The existing section 3K of the *Crimes Act 1914* recognises the need for police to be able to examine electronic equipment at another location and accordingly permits an executing officer to move a thing to another place

where 'it is significantly more practical to do so' than to examine the thing at the warrant premises. It will typically be more practical to examine electronic equipment at another place where access to specialised equipment is needed to decrypt data, use of computer forensic examiners is required and the examination of the equipment will take a long time.

Under the existing legislative framework before moving the thing the officer must have 'reasonable grounds to believe that the thing contains or constitutes evidential material'. This is the same test that the executing officer or constable assisting must apply in determining whether a thing may be seized under provisions of the search warrant. If an executing officer or constable assisting genuinely holds 'reasonable grounds to believe' the thing is evidential material, then it is questionable why they would elect to move the thing for further analysis under section 3K when that are empowered to seize the item under the search warrant provision and not be subjected to time limitations for examining and processing the equipment under section 3K.

Reducing the threshold to allow a police officer to move the material away from the warrant premises for examination where he or she 'suspects on reasonable grounds' that the thing contains or constitutes evidentiary material will overcome the above conceptual problem and also provide an effective mechanism for police to search electronic equipment located on warrant premises for evidential material in circumstances where material is unable to be accessed at the warrant premises owing to encryption or where written material is in a foreign language and is unable to be understood. A police officer may be able to establish the requisite suspicion to move the equipment based on prior knowledge or observations from the warrant premises. An added advantage of moving electronic equipment for the purpose of examination is that it minimises disruption associated with lengthy police presence at warrant premises whilst electronic equipment is examined.

Increasing timeframe of examination

The existing 72 hour limit for examining or processing a moved thing poses operational difficulties where it is necessary to examine a large volume of material, particularly where that material is in a foreign language, or it is necessary to search large capacity electronic storage devices. This problem is exacerbated where material is seized from multiple premises as part of the one operation, which is often the case in the investigation of terrorism offences. Operations involving multiple premises such as Operation Pendennis and Operation Neath typically require the executing officer to seek multiple extensions for the examination and processing of moved electronic equipment. This process of seeking extensions creates an administrative burden upon executing officer that takes them away from the task of examining the equipment itself.

The principle factors that influence the increasingly long time that it takes to forensically examine electronic equipment include:

- Increased frequency of police operations encountering electronic items;
- Increasing number of electronic items found at warrant premises in an operation;
- Increasing range of electronic devices which contain data - computers, 'thumb' drives, personal organisers, mobile phones, fax machines, smart cards, flash cards, digital cameras, GPS navigation units;
- Increased complexity of data storage devices;
- Increase in data storage capacity;
- Increased prevalence of security software and encryption technology; and
- Necessity to seek assistance orders for inaccessible computer systems.

The AFP welcomes proposed amendments that increase the time period for examination of a thing moved to another place from 72 hours to 14 days with provision to apply for 7 day extensions. This extended timeframe is necessary and appropriate given the ever increasing use of technology in criminal activity combined with the factors listed above.

Recent operations illustrate the point:

- In a recent counter-terrorism operation police executed 19 search warrants resulting in the seizure of over 2000 CD/DVDs from multiple warrant premises under provisions of section 3K. Each of these items was examined and as a result approximately 100 were seized as evidential material.
- In a recent child pornography investigation police seized over a terabyte of data from an offender's home.

Both of the above operations demonstrate the significant volume of data that is frequently encountered by police during the execution of search warrants.

It can be difficult to grasp the scale of these volumes, especially when presented with data storage devices such as DVDs or computer hard disks which can be held in one hand. An analogy which has been used by the AFP in Australian courts is that 4 terabytes represented in A4 pages of printed text would occupy approximately:

- 214,748 filing cabinets.
- 81,000 cubic metres.
- 32 Olympic swimming pools.
- The MCG arena filled to a depth of almost 4 metres.
- 2/3 of the office space in the AFP's new headquarters, the Edmund Barton Building.

Assistance Orders for inaccessible system

Password protection and encryption is becoming more common place. Section 3LA allows an executing officer to obtain an order that requires a person with knowledge of a computer or computer systems to assist access. Some current limitations with the existing assistance order provisions include:

- No provision to seek an assistance order after a warrant has been executed to assist with examination of electronic equipment that has been seized or moved to another location for examination under s.3K;
- No scope to seek assistance to access data stored in places other than a computer such as a USB drive or to seek assistance to convert data into an intelligible form;
- Restrictive categories of persons from whom assistance can be sought; and
- Inadequate penalty for failing to comply with assistance order.

The AFP support amendments that enhance the existing assistance orders provisions. Amendments will broaden the application of assistance orders to allow assistance orders to be issued after a warrant has been executed and expand the categories of persons from whom assistance can be sought to include a contractors engaged in services by the owner or lessee of the computer or device, a person who uses or has used the computer or device and current and former persons who are system administrators for the system including the computer or device.

These amendments reflect the increasing complexities of electronic equipment and provide appropriate mechanisms to assist police accessing such data from a wide range of persons under a court issued assistance order.

The AFP support increasing the penalty for non compliance with an assistance order from six months imprisonment to two years. Owing to the lenient nature of the existing penalty for not providing assistance under an order, in recent times a number of suspects have declined to render assistance when served with an order. The proposed increased penalty reflects the seriousness of non compliance with an assistance order and will provide the subjects of an assistance order with an incentive to assist police accessing electronic equipment.

Operating seized electronic equipment

Currently it is unclear to what extent an officer is able to operate seized electronic equipment under Part 1AA or equipment moved from warrant premises for examination to determine whether it contains data that constitutes evidentiary material. One such example is where electronic equipment such as a mobile phone is seized following an arrest and subsequent search of a person. Data constituting evidentiary material sourced from a mobile phone after seizure through SMS messages sent to the phone or voicemail messages not actually stored on the phone but stored on a computer server is an area that is particularly unclear.

The AFP support the introduction of section 3ZQV that will provide clarity on the operation of electronic equipment that has been lawfully seized. The proposed provision will allow an officer to operate equipment after seizure at any location to determine whether data held or accessible from the equipment constitutes evidential material. This includes data on the electronic equipment at the time of seizure such as photos, SMS messages and data sent to a phone after seizure. It also clarifies that the data not held on the equipment, but accessible using the electronic equipment, such as voicemail messages, emails stored on a computer server of a telecommunications company may be examined to determine whether the data constitutes evidential material.

This provision is necessary to ensure that AFP officers are able to properly analyse all material seized under Part 1AA or moved from warrant premises and obtain the best evidence to support a prosecution or prevent the commission of an offence.

Sharing of seized material with other agencies

For law enforcement to be effective in combating criminal activity that is increasingly sophisticated and transnational in nature it is vital that there be a mechanism that allows for information and evidential material to be freely shared between Commonwealth agencies, State and Territory law enforcement agencies, foreign law enforcement agencies and intelligence agencies for purposes connected with or related to law enforcement functions and activities. This is particularly important in combating organised criminal activity that is commonly transnational and multi-jurisdictional.

Currently the *Crimes Act 1914* only contains a provision that allows things seized under a warrant to be made available to officers of other agencies if it is necessary to do so for the purpose of investigating or prosecuting an offence to which the thing relates [s.3F(5)]. There is no reference as to whether such material is able to be used for wider purposes, such as the prevention of criminal activity. This gap creates an element of uncertainty as to whether material seized by law enforcement agencies can be used for a broader range of purposes other than those for which it was seized in the first instance.

The AFP support the introduction of proposed section 3ZQU into Part 1AA of the *Crimes Act 1914* that provides a comprehensive scheme for the sharing of seized material with other Commonwealth agencies, State and Territory law enforcement agencies and foreign law enforcement and intelligence agencies for a wide range of purposes such as the prevention, investigation or prosecution of an offence, proceeds of crime proceedings and the performance of all functions of the AFP under section 8 of the *Australian Federal Police Act 1979*.

This new provision will provide clarity for the AFP in relation to use of material seized under a section 3E *Crimes Act 1914* search warrant. For instance, where AFP members executing a search warrant in relation to drug importation offences seize computers as evidence in support of a

drug importation offence and the subsequent examination of the computer presents evidence in support of tax evasion related offences against the Commonwealth, under section 3ZQU the evidence can be shared with the Australian Tax Office for the purposes of investigating and prosecuting the subject of the warrant for tax evasion related offences.

C. National Witness Protection Program (NWPP)

The AFP maintains the NWPP that provides protection and assistance to people who are assessed as being at risk of suffering death, injury or significant property damage because they have given, or have agreed to give, evidence or a statement on behalf of the Crown in criminal or certain other proceedings or because of their relationship to such persons. The NWPP plays an important role in the effective operation of the Australian justice system by providing witnesses with appropriate protection.

The AFP welcomes the amendments to the *Witness Protection Act 1984* that provide greater protection and security of witnesses and other people included in the NWPP. Key amendments include:

- Extending protection to former NWPP participants and their families;
- Introduction of protection of identity of participants and AFP employees involved in the administration of the program during legal proceedings;
- Strengthened offences for unlawful disclosure of information; and
- Extending the application of the *Witness Protection Act* to include witnesses in State and Territory matters.

The amendments will increase the efficiency of the NWPP, improve the overall operations of NWPP and ensure the integrity of NWPP.

D. Criminal organisation and association offences

Schedule 4 of the Bill introduces new Commonwealth offences targeting criminal organisations and those who associate with people involved in organised criminal activity that have an extraterritorial application. The offences will criminalise:

- Associating with a person engaged in criminal activity where the association facilitates that criminal activity;
- Providing material support or resources that aid, or risk aiding, a criminal organisation to commit an offence;
- Committing an offence for the benefit of, or at the direction of, a criminal organisation; and

- Directing the activities of a criminal organisation where those activities aid, risk aiding or constitute the commission of an offence by the organisation.

The AFP welcomes the introduction of these offences that provides the AFP with a mechanism to both deter and prosecute persons involved in serious and organised criminal activity as a group.

One such organised criminal activity that the proposed offences may be utilised to combat is a global money laundering service utilised by a large number of Australian organised crime groups. The groups use an alternative remittance scheme known as “cuckoo smurfing” to launder proceeds of criminal activity.

This alternative remittance scheme involves the transfer of funds through accounts of unwitting persons who receive funds or payments from overseas for a legitimate reason such as an Australian expat sending his or her pay to an Australian account from abroad. A money remitter abroad (“controller”) enters into an agreement with a drug syndicate head to launder drug proceeds. The controller advises of details of the legitimate transactions to a laundering syndicate “co-ordinator” in Australia and this co-ordinator arranges for a collector to make deposits to the accounts of innocent agents in Australia to launder illegal drug cash. The controller subsequently releases the funds to a location of the drug trafficker’s choice anywhere in the world.

The extraterritorial criminal organisation and consorting offences will provide scope for the AFP to not only prosecute Australian syndicate money launderers, but also to extradite and prosecute syndicate members involved in the organised criminal activity who are not Australian citizens and dismantle laundering syndicates from the top down.

E. Money Laundering

New possession offence for proceeds of crime ≥ \$100,000

The AFP supports amendments to section 400.9 of the Criminal Code which introduce a higher maximum penalty of three years for offences of dealing in property that is reasonably suspected of being proceeds of crime, where the value of the proceeds is equal to or greater than \$100,000.

The AFP believes that this increased penalty more appropriately reflects the higher level of criminality involved in the possession of criminal proceeds over \$100,000.

Geographical jurisdiction for money laundering offences extended

The AFP supports the extension of the geographical jurisdiction for money laundering offences in Division 400 of the Criminal Code.

This amendment will enable a person who is not an Australian citizen to be prosecuted for a money laundering offence if that person deals with the proceeds of a Commonwealth or State indictable offence in a foreign country and there is a corresponding offence in that country.

The current more limited geographical jurisdiction for money laundering offences has frustrated the prosecution of overseas organisers of people smuggling ventures to Australia and other drug related money laundering activities.

In the case of people smuggling, overseas organisers are paid to organise the people smuggling venture to Australia. They then deal with that money, (which is proceeds of crime) and consequently launder the proceeds of Commonwealth crime. However, as the conduct often does not occur in Australia and the organisers often are not Australian citizens or Australian residents, they are currently unable to be extradited and prosecuted for the money laundering offences.

A number of money laundering investigations have revealed overseas based persons and syndicates who are aiding and abetting the laundering of money generated by criminal activity in Australia by moving cash generated from criminal activity out of Australia. These overseas based individuals provide the means for criminal groups in Australia to move proceeds of crime generated in Australia out of the country. These individuals currently achieve this with little risk of prosecution to themselves in Australia or in their home country.

F. Drug importation

The Bill introduces an expanded definition of "import" in the Division 307 Criminal Code import offences to address issues raised in the recent NSW Court of Criminal Appeal decision *Campbell v R* [2009] NSWCCA 214 in which the term "import" was narrowly defined to end where a consignment reaches its delivery address. The amended definition will include dealings with the substance in connection with its importation. This will include conduct that occurs after the consignment reaches its delivery address such as the recovery of the consignment after landing in Australia, clearance of the consignment, transfer of the consignment into storage, unpacking the consignment and arranging payment of those involved in the importation process.

This amendment will significantly enhance the ability of police to obtain evidence of import offences and improve drug import prosecutions.