Senate Legal and Constitutional Legislation Committee
Inquiry into the Telecommunications (Interception) Amendment Bill 2006

PUBLIC HEARING
Wednesday 15 MARCH, 2006

Questions on notice – Attorney-General's Department

Question 1

Is it necessary to provide access to additional agencies and to have a wider issuing authority? What support is there from the additional agencies that will be given access that these powers are necessary?

Extensive consultation with the additional agencies (including the Australian Tax Office, Australian Securities and Investments Commission, Australian Customs Service, and Australian Competition and Consumer Commission) has indicated that these agencies need access to stored communications to ensure that they can fulfil their statutory functions. Stored communications material, particularly e-mail communications, is similar in evidentiary value to the contents of a filing cabinet for each of these agencies who currently enjoy access to stored communications once they are in hard copy form.

There is extensive support from these additional agencies that access be provided to ensure the effective discharge of their statutory functions.

While telecommunications interception warrants may be issued by a judge of a court created by Parliament, or nominated Administrative Appeals Tribunal member, stored communication warrants will be issued by a magistrate, judge of a court created by Parliament, or nominated Administrative Appeals Tribunal member. This provision was designed to be both consistent with the current issuing authorities under the Interception Act and to implement the recommendation of the Blunn Report which suggested these types of warrants should be issued by at least a magistrate.

Question 2

Part 8 of the TI Act provides for the keeping and inspection of interception records of Commonwealth agencies. The amendments would be subject to the same regime. The principal features are:

- **agencies are required to keep detailed records;**
- **the Ombudsman is required to conduct inspections; and**
- **the Minister must prepare an Annual Report covering how many applications were made and warrants issued.**

Do these represent sufficient accountability for the arguably more invasive interception contemplated by this legislation. Would the establishment of a Parliamentary Inspector to oversee the TI Act – or at least those provisions applying to third parties – provide the required protection, particularly in view of the Ombudsman's exponentially increasing workload?

The Interception Act is replete with accountability measures and safeguards.

There is no information that suggests the Ombudsman is not capable of performing the independent oversight role. Establishing another body would be likely to involve even more resources and would create duplication. Resource allocation to the Ombudsman is of course a matter that will be subject to the usual budget processes. The important role of the Ombudsman and the other safeguards detailed below provide a comprehensive accountability framework.

The foundation of the Interception Act is subsection 7(1) which, subject to limited exceptions, prohibits a person from intercepting a communication passing over the telecommunications system. Subsection 6(1) defines interception as consisting of listening to or recording, by any means, a communication in its passage over the telecommunications system without the knowledge of the parties.

The most significant of the exceptions to the prohibition against interception is that contained in paragraph 7(2)(b), which provides that the prohibition against interception set out in subsection 7(1) does not apply in relation to the interception of a communication under a warrant. The Interception Act contains numerous provisions controlling the issue and revocation of warrants, the scope of the authority conferred by warrants, the execution of warrants and the use of information obtained under warrants. The reporting obligations under the Interception Act relate principally to Part 6 warrants; that is, those warrants issued to law enforcement agencies under Part 6 of the Interception Act.

Interception warrants

a. Serious offences

Part 6 of the Interception Act provides for the issue of warrants to the Australian Federal Police, the Australian Crime Commission and participating State law enforcement agencies.

A telecommunications interception warrant may authorise the interception of a telecommunications service in connection with the investigation of a serious offence. Schedule 4 of the Bill removes the distinction between class 1 and class 2 offences and redefines the offences which currently fall within those categories as ‘serious offences’. In most cases it is a requirement that the offence be punishable by imprisonment for life or for a maximum period of at least 7 years.

These offences include murder, kidnapping, narcotics offences, terrorism offences, serious offences involving loss of life or serious personal injury, or serious risk of such loss or injury; serious damage to property in circumstances endangering a person’s safety; serious arson; trafficking in prescribed substances; serious fraud; serious loss to the revenue of the Commonwealth or a State or the Australian Capital Territory; bribery or corruption of or by an officer of the Commonwealth, State or Territory; and child pornography offences; money laundering offences; offences relating to people smuggling with exploitation, slavery, sexual servitude and deceptive recruiting; and cyber crime offences.

b. Applying for Part 6 warrants

Applications for warrants for law enforcement purposes may only be made by the Australian Federal Police, the Australian Crime Commission, or an 'eligible authority' of a State or the Northern Territory in relation to which a declaration under section 34 of the Interception Act is in force. The Interception Act defines eligible authorities to be the police forces of each of the States and of the Northern Territory. At the commencement of the reporting year, eligible authorities also included the Independent Commission Against Corruption, the New South Wales Crime Commission, the New South Wales Police Integrity Commission, the Queensland Crime and Misconduct Commission, the Inspector of the Police Integrity Commission, the Western Australian Corruption and Crime Commission and the Parliamentary Inspector of the WA CCC.

c. Issuing of warrants

In deciding whether to issue a warrant, the Judge or nominated AAT member must be satisfied of the matters set out in warrant provisions - sections 46 or 46A of the Act as amended by the Schedules 2, 3 and 4 of the Bill.

The principal matters that the Judge or nominated AAT member is required to consider are:

- there are reasonable grounds for suspecting that a particular person is using, or is likely to use, the telecommunications service, and
- information that would be obtained by interception would be likely to assist in connection with the investigation by the agency of the seven year offence, in which the suspect is involved.
- how much the privacy of any person would be likely to be interfered with by the interception, and
- the gravity or seriousness of the offences being investigated, and
- how much the intercepted information would be likely to assist with the investigation by the agency of the offence, and
- to what extent alternative methods of investigating the offence have been used by, or are available to, the agency, and
- how much the use of such methods would be likely to assist in the investigation by the agency of the offence, and
- how much the use of such methods would be likely to prejudice the investigation by the agency of the offence.

Safeguards and controls contained in the Interception Act

The Interception Act contains a number of safeguards and controls in relation to interception.

The Australian Federal Police and the Australian Crime Commission are required to maintain records relating to interceptions and the use of intercepted information, and the Interception Act requires that the Ombudsman conduct regular inspections of those records.

In addition, a General Register of Warrants, the responsibility of which will be transferred from the Australian Federal Police to the Attorney-General's Department under Schedule 5 of the Bill, must be provided to the Minister every three months providing details of all warrants in force during the preceding three months.

Further, records of intercepted information which are not required for a permitted purpose must be destroyed after the Minister has inspected the General Register of Warrants. The Interception Act also ensures that the Attorney-General, as the Minister administering the Interception Act, is kept informed of the agencies' activities by means of reports from the agencies and the Ombudsman.

The imposition of parallel requirements by State legislation on a relevant eligible authority of the State is a precondition to the Attorney-General making a declaration under the Interception Act in relation to such an authority. If the Attorney-General is satisfied that the relevant State's legislation no longer satisfies those requirements, he may revoke the declaration.

All law enforcement agencies capable of applying for the issue of interception warrants therefore operate under equivalent supervisory and accountability provisions, including those relating to inspection and reporting.

Accountability provisions

The Interception Act contains a number of provisions designed to enhance the accountability of the agencies intercepting under warrant. The most significant of these provisions are outlined below.

a. Strict restrictions on use and disclosure of intercepted material

Consistent with the framework of the Interception Act, the use and disclosure of intercepted material is governed by a general prohibition subject to limited exceptions. Contravention of the general prohibition against use and disclosure of intercepted material is subject to a penalty of a period of imprisonment of up to 2 years.

The exceptions to the general prohibition against use and disclosure of intercepted material are specifically designed to enable the use of the material for the purposes of the investigation of criminal offences. Accordingly, the primary exception for the use and disclosure of intercepted material is in relation to the permitted purpose of

interception agencies. Each agency may use or communicate intercepted material for the specifically listed permitted purposes of that agency in relation to the investigation of serious or prescribed offences (see section 5). Generally speaking, use and communication of intercepted material for a permitted purpose is limited to a purpose in connection with the investigation or prosecution of an offence that is punishable by three years imprisonment or more. Permitted purpose includes the investigation by that agency of a relevant offence, the decision of whether or not to commence a relevant proceeding, or the communication of the intercepted material to another (listed) agency with responsibility for the relevant offence.

Other exceptions include communication of intercepted material for the purposes of a prosecution, an exempt proceeding, or a mutual assistance request.

b. Minister to inspect General Register

As amended by Schedule 5 of the Bill, the Interception Act will require the Secretary of the Attorney-General's Department to maintain a General Register showing particulars of all Part 6 warrants. The particulars required to be recorded in the Register are:

- the date of issue and period for which the warrant is to be in force;
- the agency to which the warrant was issued and the Judge or nominated AAT member who issued the warrant;
- the telecommunications service to which the warrant relates;
- the name of the person specified in the warrant as the person using or likely to use the telecommunications service;
- each serious offence in relation to which the Judge or nominated AAT member who issued the warrant was satisfied on the application for the warrant; and
- for named person warrants, the name of the person to whom the warrant relates and each telecommunications service that is specified in the warrant, or in relation to which interceptions authorised by the warrant have occurred.

The Secretary will be required to deliver new entries on the General Register to the Attorney-General every three months. Compilation of the Register involves real-time review of warrants by the Department to ensure warrants are issued in accordance with the Interception Act.

c. Minister to inspect Special Register

Similar to the requirement to maintain the General Register, the Interception Act, as amended by Schedule 5 of the Bill, will require the Secretary of the Attorney-General's Department to maintain a Special Register recording the details of warrants which do not lead, directly or indirectly, to a prosecution. The Secretary will also be required to provide the Special Register to the Attorney-General every three months.

d. Minister to be given copies of warrants and revocations and reports on outcomes

The effect of section 94 and subsection 35(1) of the Interception Act is that a copy of each warrant issued to any agency and of each instrument revoking a warrant must be given to the Attorney-General as soon as practicable. The same provisions also require that, within 3 months of a warrant ceasing to be in force, a written report about the use made of information obtained by interception under the warrant be given to:

- in the case of warrants issued to the two Commonwealth agencies – the Attorney-General; and

- in the case of warrants issued to 'declared' State agencies – the relevant responsible Minister, who must give a copy of the report to the Commonwealth Attorney-General as soon as practicable.

Agencies must also provide the Minister with the information that is required to be included in the Annual Report to Parliament.

e. Reports by carrier

Section 97 requires that the Managing Director of a carrier whose service is intercepted under a warrant report to the Attorney-General within 3 months of the warrant ceasing to be in force. The report must include details on the nature and timing of acts done by the employees of the carrier to effect interception under the warrant, and to discontinue interception when the warrant expires or is revoked.

f. Reports by Ombudsman

Under Part 8 of the Interception Act, the Commonwealth Ombudsman has the function of inspecting the records of the Australian Federal Police and the Australian Crime Commission and reporting to the Attorney-General. Eligible authorities of a State may acquire 'declared' status only where the law of the relevant State provides for inspections and reports by an agency which is independent of the eligible authority and which has sufficient powers to inspect the records of the authority. In most cases, this means the Ombudsman for the jurisdiction.

The reports of the inspections of the declared State agencies are given to the responsible State Minister who then passes a copy to the Attorney-General. The reports of the inspecting authorities to date indicate a high level of compliance with relevant statutory requirements.

Reporting requirements were amended by the passage of the *Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Act 2005*. The Act amended the Interception Act to require the Commonwealth Ombudsman to include in its annual report to Parliament a summary of the telecommunications interception inspections conducted in the relevant year together with a summary of any deficiencies identified and any remedial action taken. From the 2005-06 reporting year, the Attorney-General will be including a summary of the information received from the Ombudsman in the Telecommunications Interception Annual

Report.

g. Annual Report tabled by Attorney-General

The Interception Act requires that the Attorney-General table in Parliament a report setting out the information required by Division 2 of Part 9 each year.

Question 3

It has been suggested that an additional privacy safeguard for the B party warrants would be the requirement that the warrant cease once the service being used by the A Party has been identified. Was this provision considered?

This privacy safeguard is already provided for in the Interception Act. As with all interception warrants, the Interception Act, in accordance with section 52, requires the revocation of a warrant where the grounds upon which the warrant was issued cease to exist. The grounds for a B-Party warrant will cease to exist when it becomes possible and practicable to intercept the identified telecommunications service of the suspect or person of interest. Therefore, when there are no longer grounds for the existence of the B-Party warrant, that warrant must be revoked and a new telecommunications interception warrant must be applied for by an interception agency.

To impose further limitations on the revocation of B-Party warrants would make the legislation too inflexible in many circumstances. Identification of the service being used by the A-party may not always provide an effective alternative for interception.

Further, as with all interception, interception under the B-Party amendments will be subject to strict controls and is only available for to law enforcement and security agencies in the investigation of the most serious crimes as discussed above in response to Question 2.

Specifically, as outlined in items 3 and 9 of Schedule 2 of the Bill, a B-Party warrant will only be issued to an agency where an agency believes it is necessary to intercept the communications of an associate of a suspect, and the agency is able to demonstrate that it has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the suspect, or it is not possible to intercept the telecommunications of the suspect.

In addition, as per the existing interception regime requirements for the issuing of a warrant under Part 6 of the Interception Act, an interception warrant will only be granted to an agency when an eligible judge or nominated AAT member is satisfied:

- there are reasonable grounds for suspecting that a particular person is using, or is likely to use, the telecommunications service, and
- information that would be obtained by interception would be likely to assist in connection with the investigation by the agency of the seven year offence, in which the suspect is involved.

The eligible judge or nominated AAT member must also have regard to the following additional factors:

- how much the privacy of any person would be likely to be interfered with by the interception, and
- the gravity or seriousness of the offences being investigated, and
- how much the intercepted information would be likely to assist with the investigation by the agency of the offence, and
- to what extent alternative methods of investigating the offence have been used by, or are available to, the agency, and
- how much the use of such methods would be likely to assist in the investigation by the agency of the offence, and
- how much the use of such methods would be likely to prejudice the investigation by the agency of the offence.

In addition, B-Party interception will be subject to the same stringent reporting and oversight requirements of the interception regime, namely

1. recording the particulars of each use, recording and communication of intercepted material
2. restrictions on the use of intercepted material
3. reporting to the Attorney-General regarding the effectiveness of the interception
4. oversight of the record-keeping and reporting requirements by the Ombudsman of the jurisdiction

These reporting and oversight requirements are explained in more detail in the above response to Question 2.

Question 4

Where did the request for B-Party interceptions originate? Would you provide greater detail of the rationale for the B-Party warrant proposals: in particular, can you identify the limitations of existing named party warrants issued pursuant to the Crimes Act?

- **In evidence to the Committee, witnesses pointed to several examples including cases of a person of interest using multiple SIM cards, or instances of the need to access communications of an undercover officer.**
- **Are you able to provide the numbers of cases in which law enforcement agencies have been unable to proceed due to the limitations of existing warrants?**

- **In instances such as those referred to in the transcript – the chemical store (p. 46) or the undercover operative (p. 44) – what is to prevent the use of a consent regime, whereby the owners of the chemical store and the undercover operative give their consent to having their phones tapped for a stated period?**

The recognition of the need for B-Party warrants was identified in the *Report of the Review of the Regulation of Access to Communications* (Blunn Report). Specifically at pages 75 and 76 of the Blunn Report, Mr Blunn notes that law enforcement and security agencies raised the issue of B-Party interceptions.

Further, Mr Blunn notes the Federal Court case of *John Flanagan v The Commissioner of the Australian Federal Police* which upheld the validity of a B-Party warrant which was issued under the current warrant provisions of the Interception Act.

The Department agrees that the legal position in relation to B-party intercepts is not free from doubt, as recognised in the Blunn Report, but recognises that the Flanagan case can be used to justify an interpretation of the warrant provisions of the Interception Act to allow law enforcement to currently obtain a B-Party warrant.

Schedule 2 of the Bill expressly provides for B-Party interception on the face of the Interception Act and imposes an additional test and a 45 day limit on the issuing of a B-Party warrant.

During the development of the Bill, security and law enforcement agencies identified the need for B-Party interception and provided the following operational examples of where a B-Party warrant would be used to assist in the investigation of a serious offence:

Example 1: Attempted Murder
After the attempted murder of a female police officer, police intercepted the communications of the immediate family and girlfriend of the offender in order to assist apprehending the offender who was regarded as posing a risk to the community. The police were able to intercept the communications of immediate friends and family based on s7(5) of the Interception Act, which allows communications to be intercepted with the consent of the person who the communication is directed at where there is serious risk of personal injury. The emergency provisions proved ineffective as the family and the girlfriend had to consent to the interception of their communications which involved the disclosure of the police operation and therefore jeopardise the investigation and related operations being undertaken by the police. A named person warrant could not be obtained in this circumstance as the telecommunications services which the suspect is using are unknown and therefore cannot be intercepted.

Example 2: Crimes of Racial Hatred
Police are currently investigating a number of gang related instances which have both incited racial hatred and resulted in the infliction of serious and grievous bodily injury. Police are currently attempting to identify the services of persons of interest in relation to this matter in order to apprehend the offenders and prevent further crimes

of this nature. At this stage, the police are having little success in identifying the services of the persons of interest. Ideally, the police would like to introduce an undercover operative whose communications can be intercepted. However, the undercover operative cannot consent to having the calls monitored, as both parties must have knowledge that their phone calls are being intercepted. In this instance a B-party warrant would enable the undercover operative's communications to be intercepted, and the A-party's services to be identified. Further, a named person warrant cannot be obtained as the suspect is not using the service of the undercover operative. In addition, the undercover operative is not committing a serious offence as the operation is a controlled operation and currently telecommunications service warrants and named person warrants can only be issued where a person is involved in the commission of a serious offence.

Example 3: Gang related serious threat to life and extortion
A person who was targeted by a gang had a 'fine' of $30,000 imposed on him after being seriously assaulted. The victim knew one gang member by his nickname and fully expected to be further assaulted unless he could provide the money. The gang was very well organised and neither the identity of the gang members or their services could be identified. In this instance, the only practicable means of identifying the gang members and their services would have been by way of a B-party warrant allowing interception of the victim's communications. At times, it is better to intercept communications without the knowledge of the victim so that the offenders can be identified without the victim overreacting or making enticing comments or seen to attempt to entrap the suspect. . A named person warrant could not be obtained in this circumstance as the telecommunications services which the suspect is using are unknown and therefore cannot be intercepted. Further, a named person warrant cannot be used to tap the phone of a B-Party because the suspect is not using the B-Party's service as required under section 46A of the Act.

Example 4: Drug Trafficking and Murder
Two women, who were arrested for drug trafficking, escaped police custody and are believed to have entered into a contract to kill a member of an organised crime gang. It has been determined that the women have consistently contacted a phone number in Western Australia, however, as the service belongs to a 'B-Party', there is currently no way to intercept the communications and determine the service being used by the women, which could reveal the whereabouts of the women and prevent the commission of further crimes. Under the current warrant provisions of the Act, a named person warrant cannot be obtained as the suspects are not using the B-Party service, they are merely contacting the B-Party service. Further, it is unknown whether the B-Party is committing a serious offence and currently telecommunications service warrants and named person warrants can only be issued over a service where a person is involved in the commission of a serious offence.

Example 5: Kidnapping
A line of inquiry into the disappearance of an 18 month-old girl, who disappeared from her bedroom, revealed that a cousin of the father may be in contact with a person suspected of committing the crime, but the cousin is not suspected of being a party to the disappearance. Currently, the services used by the suspect are unidentifiable. B-Party interception would be extremely beneficial in this investigation as it would allow police to intercept the services of the innocent party to obtain information

leading to the location of the missing girl. This is currently not allowed the current warrant provisions of the Interception Act as the innocent party is not committing a serious offence, nor is the suspect using the service of the B-Party.

Example 6: Re-birthing of Motor Vehicles
This investigation relates to a large re-birthing racket of motor vehicles. Police were alerted to the racket by an associate to the persons of interest who is reluctant to supply police with the identity of persons involved in the commission of the crime or their communication services. The only possible way to effectively investigate the matter is to initially intercept the services of the associate in order to identify the persons of interest and the services that they are using.

Consenting to interception

The foundation of the Interception Act is subsection 7(1), which, subject to limited exceptions, prohibits a person from intercepting a communication passing over the telecommunications system. Subsection 6(1) defines interception as consisting of listening to or recording, by any means, a communication in its passage over the telecommunications system without the knowledge of the parties.

A person cannot only consent to having their telecommunications intercepted where all parties to the communication have knowledge that their communications will be intercepted. This would involve notifying every person who communicates with a particular service that their communications will be intercepted. In police operations, this would jeopardise the investigation of a serious offence as it would notify the suspect or person of interest that they were being investigated by the police.

Named person warrants under the Interception Act

A named person warrant under existing sections 45A and 46A authorise the interception of all telecommunications services operated by a particular person, in connection with the investigation of a Class 1 or Class 2 offence (respectively). Once the initial warrant is provided by an issuing authority, an agency is authorised to intercept all telecommunications services of the person eg. mobile phones, land line, e-mail accounts, PDA etc. The interception agency must still identify each service to enable the telecommunications carrier to execute the interception.

Named person warrants are of great value when an interception agency is investigating a person of interest who holds multiple telecommunications services and uses those multiple services in quick succession to conduct criminal enterprises. Named person warrants do not however assist in the investigation of a suspect whose telecommunications services cannot be identified (either because they do not use their own telecommunications service, or because they use a variety of services/communications equipment to conduct criminal enterprises).

For completeness, the Department notes that a person uses a telecommunications service from which they initiate or receive a communication, but do not use a telecommunications service with which they are in contact. For example, if a son calls his mother, the son is **using** his phone service and the mother is **using** hers - neither the son nor the mother is using the telecommunications service being operated

by the other. This is an important distinction to make to ensure there are no misconceptions that a named person warrant would cover the described B-Party scenarios because the suspect (A) is not using the service being operated by B. If this misconstrued construction of **use** were to be adopted, a named person warrant would authorise the interception of any telecommunications service that is likely to be contacted by the named person - this is not the case.

Question 5

Have you relied on any overseas precedent with B-Party warrants and how they have been used? Are you familiar with any?

Canada: Section 185 of the *Criminal Code of Canada* provides that an application for interception must be supported by an affidavit detailing, among other things, the type of private communication proposed to be intercepted and the names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence. Our Canadian counterparts have advised that the Code enables interception of the communications of a person who is innocent of crime provided there is a link to the crime being investigated

.

Section 184.2 of the *Criminal Code of Canada* also enables B-Party communications to be intercepted with consent of either the person making or receiving the call where there are reasonable grounds to believe that an offence against an Act of Parliament has occurred.

UK: Sections 5-8 of the *Regulation of Investigatory Powers Act 2000* provide for the warranted interception of anyone if it is in the interests of preventing and detecting serious crime, safeguarding national security and the economic well-being of the UK. The Act does not restrict the target of the warrant to persons suspected of a crime. If it can be demonstrated that a case is sufficiently justifiable, proportionate and necessary, B-Party interception would be permissible.

Sweden: Chapter 27 of the *Swedish Code of Judicial Procedure* provides that permission to intercept telecommunication may only be granted by a court (except for in emergency cases where the permission in certain cases may be preliminary granted by a prosecutor). Several prerequisites must be fulfilled for allowing interception. In sum, interception is only allowed for criminal investigation of certain offences and if the measure is of exceptional importance to the inquiry. The measure must relate to a telecommunication address held by the suspect, or an address that may reasonably be used by the suspect. However, if there are extraordinary reasons to believe that a suspect otherwise may contact a telecommunication address (in other words, interception of the "B Party" to a call), the measure may relate to such address.

United States: The Department's counterparts in the United States have advised that an interception warrant can be granted over a number of persons including all associates. The legislation which authorises interception in the United States is the *Wiretap Act* (known as 'Title III') 18 U.S.C. §§ 2510-22.

Question 6

Would it be problematic for this legislation to expressly state that schedule 2 does not override legal professional privilege?

The Interception Act would be unworkable if it were to be construed as not authorising the interception of communications subject to legal professional privilege. It would frustrate that legislative purpose if warrants could not be relied on to intercept a particular category of communications that is incapable of identification either before or at the time of the interception.

This position was affirmed in *Christopher John Carmody v Paul Stephen Mackellar & Ors* [1997] 839 FCA (30 July 1997). In that case the Federal Court held that legal professional privilege is excluded, by necessary implication, under the warrant provisions in the Interception Act. The effect of the decision was not to abrogate legal professional privilege - rather, the case provides authority for the proposition that the Interception Act authorises recording of communications which may attract legal professional privilege. Whether a communication recorded in this manner will attract legal professional privilege is a matter that is ultimately arbitrated by the courts when a prosecutor seeks to adduce those recordings in evidence.

It is important to note that investigative agencies are generally aware of the importance of ensuring that people are able to obtain advice in relation to their legal rights. As such, the Department is informed that investigative agencies will generally try to conduct a monitoring operations in a way that minimises the risk of intercepting privileged communications and will generally ensure that if a privileged communication is monitored the material obtained will be treated in the appropriate manner.

Based on the decision in Carmody described above, legal professional privilege may be upheld by a court in relation to communication recorded under a telecommunications interception warrant.

Question 7

The Law Council of Australia considers (at p. 6 of the transcript) that the bill's use of the term 'serious contraventions' (proposed Section 5E) is unacceptably wide and should be replaced by the term Class 1 Offences. Can you provide the rationale for this provision?

The definition of ‘serious contravention’ in clause 5E in item 2, at Part 1 in Schedule 1 of the Bill only applies to the issuing of a stored communications warrant. The definition of a serious intervention includes an offence which carries a penalty of at least 3 years imprisonment or a fine of 180 penalty units if the offence is committed by an individual, or a fine of 900 penalty units, if the offence is committed by a non-individual.

Consistent with the covert nature of access to stored communications, such as the three year threshold provided for in the *Surveillance Devices Act 2004*, the Bill lifts

the threshold for access from that of general search warrants and administrative notices to a three year threshold or pecuniary penalty equivalent.

A stored communications warrant provides an enforcement agency access to stored communications which are held by the carrier. A stored communications warrant only provides access to those communications in existence at the time that the warrant is executed. In this sense, stored communications warrants will give a historic snapshot to any stored communication held by a telecommunications carrier at the time the warrant is executed. A subsequent stored communications warrant can only be obtained three days after the initial warrant is executed. This ensures that a stored communications warrant cannot be executed repeatedly to provide ongoing access to those communications.

Ongoing access to telecommunications is only available with a telecommunications interception warrant. A telecommunications interception warrants give access to all telecommunications (eg. traditional telephony, e-mail, SMS) in real-time for up to 90 days and are only available to interception agencies including Australian Federal Police, the Australian Crime Commission, Independent Commission Against Corruption, the New South Wales Crime Commission, the New South Wales Police Integrity Commission, the New South Wales Police, the Victorian Police, the South Australian Police, the Tasmanian Police, the Western Australian Police, the Western Australian Corruption and Crime Commission and the Australian Security Intelligence Organisation.

Interception agencies may only apply for an interception warrant when they are investigating a serious offence. A serious offence, as amended by Schedule 4 of the Bill, is an offence which generally carries a sentence of at least 7 years imprisonment.

The difference in threshold is commensurate with the different levels of access provided by these two warrant regimes.

The setting of these thresholds is a policy matter for the Attorney-General and the Government.

Question 8

What provision has been made for increasing the level of funding to the Commonwealth Ombudsman commensurate with the expanded roles envisaged by the bill?

During the development of the Bill, the Department liaised with the Ombudsman in relation to the oversight role of the Ombudsman in the stored communications regime.

The provision of increased funding for the Commonwealth Ombudsman in order to commensurate with the expanding rile envisaged by the Bill is a matter for the Government's budget process.