GOVERNMENT RESPONSE

to

The Senate Legal and Constitutional Legislation Committee Report

on the

Provisions of the Telecommunications (Interception) Amendment Bill 2006

GOVERNMENT RESPONSE TO THE SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE REPORT ON THE PROVISIONS OF THE TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT BILL 2006

EXECUTIVE SUMMARY

The Telecommunications (Interception) Amendment Bill 2006 (the Amendment Bill) was referred to the Legal and Constitutional Legislation Committee for inquiry on 1 March 2006 for report by 27 March 2006.

This response addresses each substantive recommendation.

SUBSTANTIVE RESPONSE TO EACH RECOMMENDATION OF THE REPORT

Recommendation 1 – The Committee recommends that the Bill be amended to include a provision amending Section 280 and subsections 282(1) and (2) of the Telecommunications Act 1997, effective from the same date as the Bill, to make it clear that covert access to stored communications is not permitted without a stored communications warrant.

Government response to Recommendation 1: Accepted in part

The Government agrees that there should be no ambiguity surrounding access to stored communications. A general prohibition on accessing stored communications was implemented in the Telecommunications (Interception) Amendment Bill 2006 (the Amendment Bill) and can be found in Section 108 of the *Telecommunications (Interception and Access) Act 1979* (the Interception Act).

To remove any uncertainty surrounding the relationship between the Stored Communications Warrants regime in the Interception Act, and other legislative powers of access arising from search warrant or notice to produce provisions, the Bill was amended to insert Section 108(1A). This provision clarifies the fact that covert access is only available by means of a Stored Communications Warrant under the Interception Act. Other mechanisms require written notice to be given to the sender or recipient of the communication and thus cannot operate covertly.

The Blunn Report has separately recommended the transfer of sections 282 and 283 *Telecommunications Act 1997* (the Telecommunications Act) to the Interception Act. Implementation of this recommendation would create a single regulatory framework for access to telecommunications data for security and law enforcement purposes.

Recommendation 2 – The Committee recommends that the enforcement agencies able to access stored communications should be limited to those agencies eligible under the existing arrangements for telecommunications interception.

Recommendation 3 – The Committee recommends that the Bill be amended to permit stored communications warrants to be issued only in relation to criminal offences.

Government response to Recommendations 2 and 3: Not accepted

The Government has implemented a separate regime for access to stored communications to reflect technological developments in the storage of documents, and different privacy impacts. The new regime clarifies and centralises access arrangements for a range of enforcement (criminal-law enforcement, civil penalty-enforcement and public revenue) agencies, which have previously accessed to stored documents via a range of different warrant and notice to produce provisions.

It is not agreed that access to stored communications should be limited to intercepting agencies under chapter 2 of the Interception Act. The wider group of civil penalty enforcement and public revenue protection agencies have a legitimate need to access these types of information to enable effective investigations. This reflects the reality that the growing dominance of electronic communications in all forms of business and personal transactions displaces and renders obsolete agencies' earlier powers of access to paper documents.

However, this access is subject to controls. In particular, stored communications warrants may only be granted in relation to investigations into a contravention of a law of the Commonwealth, a State or a Territory that is:

- a serious offence (the existing threshold for obtaining a telecommunications interception warrant, as defined by section 5 of the Interception Act);
- an offence punishable by imprisonment for a period, or a maximum period, of at least three years, or the equivalent pecuniary penalty (which is at least 180 penalty units for individuals or at least 900 penalty units for corporations); or
- a breach of a civil penalty provision that would render the person committing the contravention liable to a fine of at least 180 penalty units (or at least 900 units if the person is a corporation).

In accordance with section 4AA of the *Crimes Act 1914*, 180 penalty units is equivalent to $19,800 and 900 penalty units is equivalent to $99,000.

Recommendation 4 – The Committee recommends that the Bill be amended to require applications for stored communications warrants, and the warrant itself, to include information that clearly identifies the person who will be the subject of the warrant and the telecommunications for which access is sought.

Government response to Recommendation 4: Accepted in part

The form and content of a stored communications warrant were specified by the Telecommunications (Interception) Amendment Regulations 2006 (No. 1) made on 2 June 2006. The Regulations require the person to whom the warrant applies to be fully identified. Where the person's name is not known there is scope for a telecommunications service to be identified.

Recommendation 8 – The Committee recommends that the Bill be amended to allow issuers of stored communications warrants to have regard to the length of time stored communications may have been held on a carrier's equipment and whether the communications sought can be sufficiently identified in order to minimise the impact on privacy.

Government response to Recommendation 8: Not accepted

There are a number of matters which an issuing authority must consider before issuing a stored communications warrant including:

- how much the privacy of any person would be likely to be interfered with by accessing stored communications,
- the gravity of the alleged conduct,
- how much information would be likely to be obtained,
- what other methods have been used or are available to the agency, and
- how much the use of other methods would prejudice the investigation by the agency.

It is considered that these existing privacy considerations are sufficient when balanced with the community expectation that security and enforcement organisations will investigate serious offences.

Recommendation 9 – The Committee also recommends that the Bill be amended to require issuers of stored communications warrants to consider whether stored communications are likely to include communications the subject of legal professional privilege and whether any conditions may be implemented to prevent the disclosure of such communications.

Government response to Recommendation 9: Not accepted

The Government does not agree that an issuing authority should pre-empt a decision of a court in determining whether certain communications will or will not attract legal professional privilege.

The Government considers that it is impractical and inappropriate to require an assessment of whether communications may attract legal professional privilege in seeking a stored communications warrant. This proposition was recognised by the Full Federal Court in *Carmody v Mackellar* ([1997] 839 FCA).

Recommendation 10 – The Committee recommends that the Bill be amended to specify time limits within which an agency must both review their holdings of information accessed via a stored communications warrant and destroy information as required under the proposed section 150.

Recommendation 5 – The Committee recommends that the Bill be amended to allow issuing authorities to only include those currently able to issue interception warrants.

Government response to Recommendation 5: Accepted for further consideration

With the implementation of the stored communications warrant regime, it is necessary to expand the number of issuing authorities available for enforcement agencies to obtain a warrant where this is necessary. The ability for State Magistrates to be appointed as an issuing authority provides these additional resources, and parallels arrangements for general search warrant applications.

The Government accepts that there should be further consideration of this recommendation following a reasonable operational timeframe of the stored communications regime.

Recommendation 6 – The Committee recommends that, consistent with the existing arrangements for telecommunications interception, immediate action be taken to ensure the enforceability of the stored communications provisions on State and Territory agencies by requiring complimentary legislation to be enacted as a precondition to being granted the powers of an enforcement agency under the stored communications regime.

Recommendation 7 – The Committee also recommends that as an interim measure, the definition of an enforcement agency in the Bill be amended to allow for the ability to exclude an agency specified in the Telecommunications Interception Regulations from being able to obtain a stored communications warrant.

Government response to Recommendation 6: Accepted in part

The Interception Act provides oversight mechanisms for the stored communications regime in relation to all agencies that access stored communications by expanding the functions of the Commonwealth Ombudsman considerably to:

- inspect Commonwealth and State enforcement agencies records and report to the Minister regarding compliance with the Interception Act;
- do anything incidental or conducive to the performance of these functions; and
- communicate any accessed information to a State inspecting authority if it is relevant to the performance of the State inspecting authority's functions.

The Government considers these protections adequate for the proper operation of the Act, and does not accept that complimentary State or Territory legislation should be a pre-condition for access to stored communications. As such, the Government also does not accept the need for the interim measures proposed at Recommendation 7.

However, the Government accepts that there should be further consideration of this recommendation following a reasonable operational timeframe of the stored communications regime.

Government response to Recommendation 10: Not accepted

Agencies are required to destroy information obtained via a stored communications warrant as soon as the chief officer of the agency is satisfied that the information is not likely to be required for the purposes of an investigation being undertaken by the agency. The Ombudsman is required to inspect an agency's records to ascertain compliance with the destruction of records and report to the Minister.

Additionally, agencies are required to provide a report to the Minister that sets out the extent to which records were destroyed.

The Government considers that these provisions provide appropriate obligations relating to the review and destruction of records. Where agencies are not complying with these obligations in a timely way, it can be expected that either the Minister or the Ombudsman will comment adversely on the fact.

Recommendation 11 – The Committee recommends that the Bill be amended to require agencies and the Minister to report on the use and effectiveness of stored communications warrants in a manner equivalent to the existing reporting obligations for telecommunications interception warrants.

Government response to Recommendation 11: Not accepted

The Government considers that the reporting obligations on enforcement agencies are appropriate.

Part 3-5 of the Interception and Access Act provides that the chief officer of an agency must cause records to be kept which include information such as each warrant issued to the agency and each instrument of revocation held by the agency.

Division 2 of Part 3-5 outlines the additional functions of the relevant State and Federal Ombudsmen in relation to inspecting the records of enforcement agencies and to report their findings to the minister. The Interception and Access Act requires that the Attorney-General table in Parliament a report setting out the information required by Part 3-6 each year. Chapter 5 of this report presents the information required under the Interception and Access Act.

Division 2 of Part 3-6 requires that the report tabled by the Attorney-General contains the following, in terms of each agency, and in total:

- Applications for stored communications warrants generally
- Telephone applications
- Renewal of applications
- Warrants issued containing conditions and/or restrictions
- Effectiveness of warrants

These obligations are consistent with the nature of the access conferred by the stored communications regime.

Recommendation 12 – The Committee recommends that additional resources be provided to the Ombudsman to enable the Office to fulfil the expanded functions under this Bill.

Government response to Recommendation 12: Accepted

The government has agreed to provide additional supplementation to the Ombudsman to fulfil its increased responsibilities arising out of the stored communications warrant regime.

Recommendation 13 – The Committee recommends that the Bill be amended to extend the timeframe for section 153 reports to six months.

Government response to Recommendation 13: Not accepted

The timeframe imposed for the stored communications reporting regime is consistent with the Ombudsman's reporting obligations in relation to the telecommunications interception regime, ie by 30 September each year. However, in respect of agencies to which the telecommunications interception reporting regime does not apply, the timeframe imposed for the stored communications reporting regime means that the Ombudsman may not be able to decide which agencies to inspect until after 30 September when the agencies will have submitted their annual reports to the Minister and disclosed whether they have used stored communications warrants. For this reason it is important that all regulatory agencies co-operate to enable the reporting from the Ombudsman to take place in a reasonable period of time to ensure that any deficiencies that may impact on the integrity of the stored communications regime be identified and remedied in a timely fashion.

Recommendation 14 – The Committee recommends that the Bill be amended to ensure that copies of communications can not be accessed without a stored communications warrant.

Government response to Recommendation 14: Accepted in principle

A general prohibition on accessing stored communications was implemented in the Amendment Bill (Section 108 of the Interception Act).

The legislated stored communications access regime does not differentiate between 'copies' or 'original' stored communications. The regime applies to any communication that is not passing over a telecommunication system and is held on equipment accessed directly from a carrier. As such, no amendment to the legislation is considered necessary since the Committee's recommendation is already the legal position.

Recommendation 15 – The Committee recommends the definition of 'record' be amended so that it applies in relation to accessing a stored communication.

Government response to Recommendation 15: Not accepted

The definition of 'record' in section 5 – a record or copy, whether in writing or otherwise, of the whole or part of the information – has two parts. The first relates to 'information' and the second to 'an interception'. Since the former category includes stored communications, it is unnecessary to specifically add this to the definition.

Recommendation 16 – The Committee recommends that the issue regarding whether or not access to stored communications is accessible via the sender is settled and the Bill be amended as necessary.

Government response to Recommendation 16: Accepted

Adopted and implemented in the Amendment Act.

The definition of *stored communications* was amended to clarify that access to stored communications can be accessed via the sender or the receiver.

Recommendation 17 – The Committee recommends that prior to the passage of the Bill the definition of stored communications be amended so that the Australian Communications and Media Authority's ability to enforce the Spam Act is not limited.

Government response to Recommendation 17: Accepted

The provisions allowing Australian Communications and Media Authority officers' access to stored communications as part of their function of enforcing the *Spam Act 2003* were substantially implemented in the Bill. The Government accepts that the stored communications regime should not adversely impact upon the enforcement of the *Spam* Act, and will ensure that the regime does not impede those enforcement objectives.

Recommendation 18 – The Committee recommends that as a precondition to issuing a warrant under subsection 9(3), there must be evidence that the B-party's telecommunications service is likely to be used to communicate or receive information relevant to the particular activities prejudicial to security which triggered the warrant.

Government response to Recommendation 18: Not accepted

Security and enforcement agencies are required to specify the facts and grounds on which any warrant is sought. In addition, interception of the B-party service is only available where the interception agency can satisfy the issuing authority that the

person being intercepted will likely be contacted on that telecommunications service by the person of interest, that there is no other practicable means of identifying the services, and that interception of that service would not otherwise be possible.

One of the purposes of the B-party warrant regime is to enable the intercepting agency to identity a target's service/s where the target is communicating with a B-party through otherwise unidentifiable services. It would unnecessarily limit the effective use of this provision to restrict the availability of such warrants to circumstances where the target is using the B-party to communicate or receive information directly relevant to the activities of concern. In the circumstances where the B-party is used to identify a target service, the agency can revoke a B-party warrant seek a specific direct warrant for the target's service/s.

Recommendation 19 – The Committee recommends that the Bill be amended to require that an applicant for a B-party warrant demonstrate:

- evidence to support their belief that the information likely to be obtained from the intercept is material to the investigation; and
- establish that it cannot be obtained other than by telecommunications interception or the use of a listening device.

Government response to Recommendation 19: Accepted in principle

The Government agrees that sufficient evidence should be provided to an issuing authority to justify the issuing of a B-party warrant.

Specifically, paragraph 46(2)(c) requires the issuer of a B-party warrant to a law enforcement agency to have regard to the information provided in respect of the request for a warrant and to determine whether the information that is identified would be likely to assist in connection with the investigation.

Subsection 46(3) provides that a B-party warrant cannot be issued unless the issuer is satisfied that there are no other practicable methods available to the agency at the time of making the application or interception of communications made to or from a telecommunications service used by the person would not be practicable.

Recommendation 20 – The Committee also recommends that the proposed section 46(3) (which contains the requirement that the issuing authority must not issue a B-party warrant unless he or she is satisfied that the agency has exhausted all other practicable methods of identifying the telecommunications services used) be amended to exclude the word 'practicable', to ensure that before a person is subject to a B-party warrant no other way of approaching the problem is available.

Government response to Recommendation 20: Not accepted

The inclusion of the term 'practicable' is considered important from an operational effectiveness point of view. There may be cases where alternative methods of

identifying telecommunications services are available, but in particular circumstances, not practicable when a covert approach is required.

The issuing authority would still need to be satisfied that a B-party warrant may be issued within the restrictions of the TIA Act.

Recommendation 21 – The Committee recommends that the Bill be amended to state that B-party interception warrants cannot be renewed. If further interception is required after a warrant expires, it must be the subject of a fresh application.

Government response to Recommendation 21: Accepted in principle

The Government agrees that a B-party warrant should not be renewable.

Each application for any warrant under the Interception Act is a fresh application and must be assessed on its merits regardless of whether a warrant had been previously issued or was still in existence. If a warrant is about to expire, an agency may seek another warrant to start at the expiry of the existing warrant to ensure there is continuity in the investigation. Although the TIA Act refers to the renewal of warrants for reporting purposes, this has no relationship to the issuing requirements.

As such, it is not considered that an amendment is necessary.

Recommendation 22 – The Committee recommends that Schedule 2 be amended to provide that certain material obtained under a B-party warrant will be exempted from use under the legislation. This material should include bona-fide communications between solicitor and client; clergy and devotee; doctor and patient and communications by the innocent person with any person other than the person of interest to the law enforcement agency.

Government response to Recommendation 22: Not accepted

As noted at recommendation 9, it is the Government's position that the relevant court should determine whether certain communications will or will not be admissible in evidence.

Recommendation 23 – The Committee further recommends that the Bill be amended to introduce defined limits on the use and derivative use of material collected by B-party warrant.

Government response to Recommendation 23: Not accepted

The use and derivative use of information obtained via a B-party warrant is governed by the same strict rules as material obtained under a service or named person warrant.

The Interception Act restricts the derivative use of information obtained via any interception warrant in that an intercepting agency may only pass on the information to another agency where the information appears to relate to the commission of a serious offence which should be investigated by another agency.

The communication of interception product by intercepting agencies is subject to the oversight of the Commonwealth Ombudsman and State equivalents.

Recommendation 24 – The Committee recommends that:

- there should be strict supervision arrangements introduced to ensure the destruction of non-material content in any form;
- the number and justification of B-party intercept warrants should be separately recorded by the Agency Co-ordinator and reported to the Attorney-General; and
- the use of such warrants should be separately reported to the Parliament.

Government response to Recommendation 24: Accepted in part

The Government supports the implementation of effective reporting requirements for the communications interception regime and requires the use of B-party warrants to be separately reported within agencies' annual reports to the Attorney-General, which are required within three months of 30 June each year. This information is required to be included in the Attorney-General's annual report to Parliament that is prepared as soon as practicable after 30 June each year (section 99 *et seq*).

However, the Government notes that adding separate reporting requirements of B-party warrants to the Agency Co-ordinator who would then report to the Attorney-General would be a duplication of effort and not appropriate.

The destruction provisions in the Interception Act apply equally to B-party interception. These require the destruction of material once the general and special registers of warrants have been inspected by the Attorney-General. These registers are compiled by the Secretary of the Attorney-General's Department every three months. After they are considered by the Attorney-General, a notice is provided to all agencies, at which point they may destroy all material that is referred to in both registers (see Part 2-7). It is not considered necessary to stipulate specific supervision requirements for the destruction of material.

Recommendation 25 – The Committee recommends that the Bill should include a provision for the provisions to expire in five years, with a review at that time or earlier. The Review should encompass the broader issues surrounding the suitability and effectiveness of AAT members in the warrant issuing regime, together with consideration of ways in which the Act may be amended to take account of emerging technologies such as peer-to-peer technology.

Government response to Recommendation 25: Not accepted

In accordance with best practice regulation, the telecommunications interception regime is reviewed on a regular basis to refine the balance between security and enforcement requirements and privacy considerations. Full consideration of all the provisions within the TIA Act will be undertaken on an on-going basis.

Where it was considered appropriate, sunset provisions have been included for specific provisions in the Bill. For example, the provisions allowing measures to ensure the security of the AFP computer network, will expire two years from the date of enactment. This provides a temporary solution to an urgent operational requirement while a more permanent solution is developed.

However, the Government does not consider a sunset clause to be appropriate in relation to the wider Bill. The matters proposed in this bill do not reflect a response to a particular short-term issue that is likely to dissipate in the longer term. Rather, this legislation reflects a response to permanent changes in the law enforcement and national security environment, caused in large part by changes in technology. As such, it is anticipated that these legislative provisions will assume even greater importance in future.

Recommendation 26 – The Committee recommends that the recommendation contained at paragraph 3.2.5 of the Blunn report be adopted, and priority given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.

Government response to Recommendation 26: Accepted

The Government supports the use of unique identifiers as the basis for access to communications. General provisions have been implemented to enable interception agencies to intercept communications to and from communications equipment such as mobile handsets and computer terminals via a unique identification number. These warrants will only be issued where the requesting agency can show that the unique identifying number is indeed a unique source and that there are no other practicable methods of identifying the telecommunications service.

The Department is continuing to work with agencies and industry in relation to unique identifiers for telecommunications equipment.

Recommendation 27 – The Committee recommends that the amendments proposed in Schedule 6 of the Bill be passed.

Government response to Recommendation 27: Accepted

Schedule 6 of the Bill was passed on 30 March 2006.

Recommendation 28 – Subject to the amendments set out above, the Committee recommends that the Bill be passed.

Government response to Recommendation 28: Accepted in part

As noted, the Bill was passed on 30 March 2006. The Government has accepted the majority of the recommendations of the Senate Committee's report, with 18 of the recommendations already partly or wholly addressed though changes made to the Amendment Bill prior to passage or noted for future consideration.