Parliament of Australia
Department of Parliamentary Services

PARLIAMENTARY LIBRARY
INFORMATION ANALYSIS ADVICE

BILLS DIGEST NO. 53, 2010–11 3 December 2010

Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010

Margaret Harrison-Smith
Law and Bills Digest Section

Contents

ISSN 1328-8091

Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010

Date introduced: 30 September 2010

House: House of Representatives

Portfolio: Attorney-General

Commencement: The day after the Act receives the Royal Assent

Links: The links to the Bill, its Explanatory Memorandum and second reading speech can be found on the Bills home page, or through http://www.aph.gov.au/bills/. When bills have been passed they can be found at the ComLaw website, which is at http://www.comlaw.gov.au/.

Purpose

The purpose of the Bill is to facilitate increased cooperation, assistance and information sharing in areas of key national security by the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO).

Background

This Bill was introduced in the 42nd Parliament but lapsed on the proroguing of the Parliament on 19 July 2010. The Bill replicates that introduced in the last Parliament.

The Bill is consistent with findings made in the 2007 'Report of the Review of Homeland and Border Security'.[1] That report was not publicly released. However the Summary and Conclusions of the Review released on 4 December 2008 pointed to:

> The increasingly enmeshed nature of foreign, defence, security and law enforcement intelligence points to the need for a single, overarching framework for national intelligence coordination and priority setting. There is also a need for a closer relationship between the Australian Intelligence Community agencies and the intelligence analysis units established within non-AIC agencies in response to newly emerging threats. In an environment in which the sharing of intelligence and data is critical, intelligence and law enforcement agencies must ensure that their relationships are seamless.[2]

1. R Smith AO PSM, *Report of the review of homeland and border security*, 27 June 2007. The report was not publicly released.
2. *Report of the review of homeland and border security: summary and conclusions*, 4 December 2008. See: http://pmrudd.archive.dpmc.gov.au/sites/default/files/file/documents/20081204_review_homeland_security.pdf, viewed 2 November 2010.

The Government's response to the report took the form of a National Security Statement made by the Prime Minister in the Parliament, also on 4 December 2008. The Statement reiterated the need identified by the review for better coordination between existing national security departments, agencies and capabilities.[3]

The Explanatory Memorandum says that the Bill also represents a response to the failed terrorist attack on North West Airlines Flight 253 on 25 December 2009.[4]

Committee consideration

The Bill has been referred to the Senate Legal and Constitutional Affairs Committee for inquiry and report by 24 November 2010. Details of the inquiry are at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommuinication_interception_intelligence_services_43/index.htm. Submissions to the Committee's inquiry are at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommuinication_interception_intelligence_services_43/submissions.htm

The Bill was reviewed by the Senate Standing Committee for the Scrutiny of Bills on 27 October 2010. Details of the Committee's report are at: http://www.aph.gov.au/Senate/committee/scrutiny/alerts/2010/d08.pdf Submissions to the Committee's inquiry are at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommuinication_interception_intelligence_services_43/submissions.htm

The views of the Scrutiny of Bills Committee and of submitters to the Senate Committee inquiry are referred to further in the Key Provisions section of this Digest.

Position of major interest groups

The Australian Federal Police Association strongly supports the Bill:

> We are confident that this proposed Bill will create a closer relationship between intelligence, enforcement and other national security agencies through removing artificial barriers to interoperability and intelligence.[5]

---

3. The First National Security Statement to Parliament, Address by the Prime Minister of Australia, Kevin Rudd, House of Representatives, 4 December 2008, p. 12555. See: http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/2008-12-04/0045/hansard_frag.pdf;fileType=application%2Fpdf
4. See for example, P Slevin, 'Fear and heroism aboard North West Airlines Flight 253 after attempted bombing', *Washington Post*, 27 December 2009, viewed 2 November 2010, http://www.washingtonpost.com/wp-dyn/content/article/2009/12/26/AR2009122601150.html
5. Australian Federal Police Association submission to Senate Legal and Constitutional Affairs Committee, p. 2, http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommuinication_interception_intelligence_services_43/submissions.htm

The Australian Commission for Law Enforcement Integrity (ACLEI) is also supportive of the Bill saying that broadening the number of agencies to which it could go for assistance in executing telecommunications warrants:

> ... would assist ACLEI to preserve the independence and integrity of corruption investigations. Specifically, this 'capability independence' would provide the advantage of distance from the agencies within the [*Law Enforcement Integrity Commissioner Act 2006*] jurisdiction, when such distance may be needed to protect an investigation from possible compromise.[6]

However the Australian Law Reform Commission (ALRC), the Office of the Australian Privacy Commission (APC), the Monash University Castan Centre for Human Rights Law (Castan Centre) and the Australian Privacy Foundation (APF) raise privacy concerns with the Bill.

There were also very strongly expressed concerns from the NSW Council for Civil Liberties, the APC, the Castan Centre and the APF about the need to keep the functions of law enforcement agencies and intelligence bodies as distinct as possible.

Additionally, in their combined submission, the Communications Alliance, Australian Mobile Telecommunications Association and Internet Industry Association (Associations) are critical of Schedule 2 of the Bill (Requirement to inform of proposed changes):

> ... the new regime ... will create delay, competitive disadvantage, uncertainty and regulatory risk to carriers/nominated carriage service providers as the regime effectively gives Agencies the right to determine what products or services a carrier/nominated carriage service provider can deploy, and when.[7]

Financial implications

The Explanatory Memorandum states that the amendments in this Bill will have no financial impact.[8]

Main issues

A principal objective of the Bill is to facilitate information-sharing between Australia's key intelligence and law enforcement agencies. There is therefore a significant issue as to whether, in seeking to do this, the Bill strikes an appropriate balance between the public interest in:

- maintaining the safety and security of the Australian community through effective intelligence and law enforcement agencies; and

6. Australian Law Enforcement Integrity Commission, submission to Senate Legal and Constitutional Affairs Committee, p. 4. http://www.aph.gov.au/senate/committee/legcon_ctte/telecommuinication_interception_intelligence_services_43/submissions.htm
7. Communications Alliance, Australian Mobile Telecommunications Association and Internet Industry Association, submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 5.
8. Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 2.

- the public interest in protecting the personal information of individuals.

The APC suggests that measures to diminish privacy should only be undertaken where:

- necessary and proportional to address the immediate need; and
- subject to appropriate and ongoing accountability measures and review.[9]

Views on this issue are further explored in the following section of this Digest.

Key provisions

The Bill has seven Schedules.

Schedule 1 — Exercise of warrant powers

This Schedule will amend Part 2-5 (Warrants authorising agencies to intercept telecommunications) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to enable the Australian Security Intelligence Organisation (ASIO) to provide technical assistance to law enforcement agencies in relation to telecommunications interception warrants issued to those agencies.

Item 3 repeals subsection 52(3) and inserts **proposed subsection 52(3).** Section 52 relates to the situation where a Judge or AAT member who issued a warrant on a telephone application revokes the warrant**.** When this happens, the section requires the chief officer of the agency to whom the warrant was issued to notify the chief officer of an agency exercising authority under the warrant 'forthwith' and to provide them with a copy of the revocation.

The effect of the amendment will be to require the Director-General of Security to be informed of the revocation of a warrant where an employee or officer of ASIO, or a person assisting ASIO in the performance of its functions, is exercising authority under the warrant.

Item 5 extends subsection 55(3) to allow the chief officer of an agency (or his or her delegate) to authorise ASIO officers or employees, or persons assisting ASIO in the performance of its functions, to exercise the authority of an interception warrant. ASIO officers and employees are not covered by the reference to agency officers and employees in current subsection (3). The subsection currently only applies to officers and employees of the agencies.

Item 7 inserts **proposed subsection 55(8)**. The new subsection will clarify that the reference in proposed paragraph 55(3)(d) to 'persons assisting [ASIO] in the performance of its functions' does not remove the responsibility of ASIO for the actions of those persons.

Item 8 repeals subsections 57(1), (2) and (3) and substitutes **three proposed subsections**. Section 57 sets out the grounds on which a warrant can be revoked, and when revocation is mandatory. It also

9. APC submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 5.

sets out the obligations of the chief officer of the agency who has revoked the warrant to notify any person exercising authority under the warrant. The new subsections will extend the application of section 57 to ASIO when it is exercising the authority under a warrant that has been revoked.

Items 10, 11, 12 and 13 extend the application of section 58 to situations when another agency (including ASIO) is exercising the authority of an interception warrant. Section 58 sets out the obligations on a person who has been notified of the revocation of a warrant under section 57 of the TIA Act. In this situation, the agency must take steps to stop the interception once informed of the revocation.

Item 16 inserts **proposed subsection 61(4A**) which will enable an evidentiary certificate to be issued by a person authorised by the Director-General of Security where a person referred to in **proposed paragraphs 55(3)(c) or (d)**) is providing assistance to a law enforcement agency in connection with a warrant executed under Part 2-5.

Item 17 will replace the current subsection 61(5) with a **proposed subsection** which confirms that a certificate under **proposed subsection 61(4A)** is also prima facie evidence.

Items 18, 19 and 22 will limit the use and disclosure of information intercepted by ASIO on behalf of another agency.

Item 18 inserts **proposed subsections 64(3) and (4**) to clarify, having regard to subsections 64(1) and (2), that ASIO, or a person assisting ASIO in the performance of its functions, is not able to use or disclose for its own purposes information obtained by interception on behalf of another agency, or otherwise providing technical assistance. Subsections (1) and (2) allow the use or disclosure of intercepted information, warrant information or foreign intelligence information in connections with ASIO's functions or for security purposes.

Item 19 proposes amendment to section 65. Section 65 presently permits the Director-General of Security to communicate intercepted information and related information in accordance with the ASIO Act. **Proposed subsection 65(3)** will provide that ASIO cannot disclose information obtained by it under a warrant conferred on it under **proposed section 55** (item 6) unless the information has been communicated to the Director-General of Security under section 68 of the TIA Act (Chief officer may communicate information obtained by agency).

Item 22 inserts **proposed subsections 67(1A) and (1B)**. The effect of these provisions will be that agencies intercepting information on behalf of, or providing technical assistance to another agency cannot use the information obtained for their own purposes, unless the information has been communicated to the Director-General of Security under section 68 of the TIA Act.

The APC is supportive of the limits imposed on the use and disclosure of information intercepted by ASIO on behalf of another agency under items 18, 19 and 22.[10]

Item 21 repeals subsection 66(2) and inserts **proposed subsections 66(2) and (3). Proposed subsection 66(2)** will permit the chief officer of an agency to authorise persons or classes of person referred to in **proposed paragraphs 55(3)(a) to (c)** to receive information obtained under warrants issued to the agency.[11]

The Explanatory Memorandum says that this:

> ... will facilitate [ASIO] or an agency conducting interception on behalf of another agency, undertaking technical assistance and then passing the information to the investigative officer within the agency which obtained the warrant.[12]

Proposed subsection 66(3) will provide that where the chief officer of an agency authorises someone outside the warrant-obtaining agency to receive the information obtained, the authorisation is only for the purpose of the investigation to which the warrant relates. The Explanatory Memorandum says that this will:

> ... maintain existing controls and safeguards in the TIA Act on dealing with intercept and related information.[13]

Items 23 and 24 propose amendments to section 81 (Other records to be kept by Commonwealth agencies in connection with interceptions). When ASIO is intercepting information on behalf of a Commonwealth interception agency, **proposed subsection 81(2A)** (item23) will require the Director-General of Security to record and provide the agency with any information it requires to meet its record keeping obligations under section 81 of the TIA Act.

Item 25 inserts **proposed section 81AA** which will make similar provision for interceptions by ASIO on behalf of a State or Territory interception agency.

Item 26 inserts **proposed paragraph 103(aca)** to ensure that details of details of the number of interceptions by ASIO on behalf of other agencies will be included by those agencies in the annual report on warrants issued under Part 2-5 of the TIA Act.

The APC supports the proposed reporting requirements under items 23 to 26.[14] However, in view of the varied application of the *Privacy Act 1988* (Privacy Act) to Australian intelligence agencies and

10. APC submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 8
11. As a result of these proposed new paragraphs, ASIO officers or employees can exercise authority under a Part 2-5 warrant.
12. Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 7.
13. Ibid., p. 8.
14. APC submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 8

Commonwealth and State law enforcement agencies covered by the Bill, varied the APC suggests the development of overarching guidelines on personal information handling practices.[15]

Schedule 2 — Requirements to inform of proposed changes

Chapter 5 of the TIA imposes obligations on the telecommunications industry to assist interception agencies. Those members of the industry subject to these obligations are carriers (owners of telecommunications infrastructure)(Cs), carriage service providers (CSPs) and nominated carriage service providers (NCSPs).[16]

Part 5-4 of Chapter 5 of the TIA (Interception capability plans) requires C/NCSPs to submit an interception capability plan (IC plan) to the Communications Access Co-ordinator (CAC).[17] An IC plan must be updated if there is a specified change which would adversely affect the ability to conduct interception, or to comply with the requirements of the TIA. Notification of the change is presently required only after a change is made.

This Schedule will insert **proposed Part 5-4A** in the TIA Act. This Part will require C/NCSPs to inform the CAC of proposed changes that could significantly affect their capacity under the TIA to assist interception agencies. The proposed changes are said to be modelled on Division 4 of Part 5 of the Telecommunications Act which was repealed in 2007. Those provisions were thought to be redundant but are not met by current IC plan proposals.[18]

Items 1 to 3 propose relocation of the definitions of 'carrier', 'carriage service provider' and 'nominated carriage service provider' to the definition section of the TIA Act, section 5, while **item 6** proposes their corresponding removal from section 194 of the Act. Because Part 5-4 and **proposed Part 5-4A** will both only apply to NCSPs, for ease of reference, **item 2** will set out when the definition of 'carrier' does not include a CSP.

Item 4 inserts a new definition of 'notifiable equipment' in section 5.

Item 8 inserts **proposed Part 5-4A — Requirement arising from proposed changes**

Proposed section 202A outlines the purpose of the new Part:

15. Ibid. The APC also recommends revision of the guidelines on personal information handling issued by the Attorney-General in 2007 under the ASIO Act.
16. The Attorney-General may nominate a carriage service provider under subsection 197(4) of the TIA Act.
17. The CAC is a statutory position created under the TIA Act. An officer of the Attorney-General's Department presently fills this role. The CAC is the primary point of liaison between interception agencies and industry and plays a major role in assisting industry members to comply with the legislative obligations to provide reasonably necessary assistance to Australian enforcement and notional security agencies: Attorney-General's Department submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 5.
18. Attorney-General's Department submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 5.

- to require C/NCSPs to give notice of any change that is proposed to a telecommunication service or system that may affect their capacity to comply with obligations under the TIA Act or section 313 of the *Telecommunications Act 1997* (Telecommunications Act);[19] and

- to allow the CAC to notify agencies of the proposed changes.

Proposed subsection 202B(1) provides that the section will apply when a C/NCSP becomes aware 'that the implementation by the carrier is likely to have a material adverse effect' on the C/NCSP's capacity to comply with its obligations under the Act**. Proposed subsection (2)** sets out specific examples of relevant changes, including the provision of new telecommunications services, changing the location of notifiable equipment or entering into outsourcing arrangements.[20]

The Associations query the point at which they would be required to notify the CAC under this provision.[21] They express concern at the proposed amendment in the context of the need to launch new and 'off-the-shelf' services and products, including those sourced from overseas, without undue delay if they are to remain competitive or even viable.[22] The Privacy Foundation also expresses uncertainty as to the scope of requirements suggesting that it:

> ... would appear to be an onerous burden on C/NCSPs to, require them unreasonably to "speculate" about the possible effect of changes and whether they might have a "material adverse effect" on capacity to comply with intercept related obligations.[23]

Proposed subsections 202B(3) and (4) will require the C/NCSP to provide the CAC with a written notification describing the proposed change.

Proposed subsection 202B(5) will permit the C/NCSP to implement the proposed change if they have not received written notification from the CAC in writing within 30 days of their having notified the change. However, **proposed subsection 202B(7)** clarifies that, notwithstanding **proposed subsection 202B(6)**, the CAC may make a Determination subsequent to the 30 day period provided for in that proposed provision.

The Associations express concern at **proposed subsection (7)**:

> ... the certainty and reasonableness that [proposed section 202B(5)] purports to offer is completely undermined by section 203B(7) which gives the CAC the power to effectively disregard any timeframes previously set out in Schedule 2 and to make a Determination at any

19. Section 313 places more general obligations on C/CSPs, for instance, to do their best to prevent telecommunications networks and facilities to be used for or in relation to the commission of offences, including the misuse of data passed over the networks. For further detail see: Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 12.
20. 'Notifiable equipment' is defined in a new definition inserted in section 5 of the TIA by **item 4** of the Bill.
21. Associations' submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 6.
22. Ibid., p. 4.
23. Privacy Foundation submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 2.

> later point in time. [24]

Proposed subsection 202B(6) will prevent the C/NCSP from implementing the proposed change where, within 30 days of submitting their change notification, the C/NCSP receives notification from the CAC and, also within that 30 day period, the CAC makes a determination under section 203 that applies to the C/NCSP.

The Explanatory Memorandum says that:

> ...if the CAC notifies a C/NCSP of a possible issue, and within that 30 day period, a solution is put in place which satisfies both the C/NCSP and the CAC, the change can be implemented before the 30 day period has elapsed.[25]

This is not specifically provided for in **proposed section 202B** although, equally, it is not precluded.

Proposed subsection 202C(1) allows the CAC to consult with agencies from which notifications have been received. **Proposed subsection 202C(2)** will require the information to remain confidential. However, this is not intended to preclude the circulation of the information within the Commonwealth Government, interception and enforcement agencies.[26]

The Associations express concern at this proposed provision, saying that no direct confidentiality obligations would be owed to them by other agencies. They say also that the Bill does not restrict the subsequent wider circulation of the information within agencies.[27]

Schedule 3 — Disclosure of telecommunications data relating to missing persons

- **Item 3** inserts **proposed section 178A** which will permit an authorised officer of the Australian Federal Police or a State Police Force to authorise the disclosure of telecommunications data the disclosure of which would otherwise be prohibited by the Telecommunications Act. **Proposed subsection (2)** permits the disclosure of information that came into existence prior to the receipt of the authorisation by the carrier from whom the disclosure is sought. **Proposed subsection (3)** will require an authorised officer to be satisfied that the disclosure is reasonably necessary to the finding of the missing person.

At present, the TIA Act only permits the interception and authorised disclosure of telecommunications data in limited circumstances for law enforcement and national security purposes. Disclosure for public safety purposes is not permitted.

The Explanatory Memorandum explains that because:

---

24. Associations' submission, op. cit., p. 7.
25. Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 13.
26. Ibid.
27. Associations' submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 7.

> ... locating a missing person relates to public safety rather than the investigating of a criminal activity, the new provisions relating to the use of information obtained to locate a missing person will be more stringent than the provisions relating to the use of information obtained to investigate criminal conduct.[28]

Item 5 inserts **proposed subsection 182(2A)** which will regulate the secondary disclosure of 'missing person' information under proposed section 178A. The disclosure must be:

- reasonably necessary for finding the missing person
- disclosed to the person who notified the police; and
- the missing person consented to the disclosure
- the missing person is unable to consent and the disclosure is reasonably necessary to prevent a threat to the persons health, life or safety; or
- the missing person is dead.

The APC favours the removal of 'reasonably' from 'reasonably necessary' in these threshold tests; the addition of 'serious' to 'threat', and the provision of greater guidance as to what constitutes 'consent'.[29] The APC also considers that secondary disclosures should be limited to whether or not the person is alive.[30]

Item 7 inserts **proposed sub-section 182(4)** which will restrict the use by police of missing person information to the location of a missing person.

The **proposed Note** to the proposed subsection says that a defendant bears an evidential burden in establishing the existence of the circumstances that would authorise the disclosure of material that would, apart from those circumstances, constitute an offence.

Item 7 also inserts **proposed subsection 182(5)** which defines 'missing person information' (information obtained under **proposed section 178A**) and 'non-missing person information' (information obtained under another provision in Part 4-1 of the TIA).

The Australian Federal Police Association considers that the Schedule 3 amendments will be of great assistance in the location of missing persons.[31] However, the APC fears 'function creep', with additional public safety exceptions being added over time[32] The APC recommends binding rules or regulations relating to the handling of the data relating to missing persons.[33]

28. Ibid., p. 13.
29. APC submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 12.
30. Ibid.
31. Australian Federal Police Association submission to Senate Legal and Constitutional Affairs Committee, p. 3.
32. APC submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 9.
33. Ibid.

I**tem 8** inserts **proposed paragraph 186(1)(aa)** requiring agencies to report annually on the number of authorisations under **proposed section 178A**. The APC considers that there should also be provision for statutory review of the proposed missing person provision after a period of operation.[34]

The ALRC considers that the TIA Act should provide that irrelevant material containing accessed telecommunications data should be destroyed when no longer needed in relation to a missing person or other permitted purpose.[35]

Item 9 provides that information or documents in existence, and missing persons notified as missing before or after its commencement will be covered by the Schedule.

Schedule 4 — Stored communications warrants in relation to victims of serious contraventions

This Schedule will amend the TIA to remove existing ambiguity as to whether or not a stored communications warrant can be obtained to access stored communications of both the offender and the victim of a serious contravention. A stored communication is one that is not passing over a telecommunication system, is held on a carrier's network and can only be accessed with the help of the carrier.[36]

Item 1 proposes to amend paragraph 116(1)(d) by adding the bracketed words 'including as a victim of the serious crime' after the words 'a serious contravention in which the person is involved'.

Item 2 inserts **proposed paragraph 116(2)(da)** which clarifies that covert access to communications is confined to when the victim cannot consent or where it is impracticable for the victim to consent.

The ALRC makes the general observation that reporting requirements for stored communication warrants should be as strong as those for interception warrants.[37]

Item 4 provides that conduct engaged in, and information accessed by warrants first held on equipment before or after the commencement of the Schedule will be covered. The Explanatory Memorandum says that the Schedule will not retrospectively criminalise any activity.[38]

---

34. Ibid., p. 13.
35. ALRC.1. See also ALRC, *For your information: Australian privacy law and practice*, Report 108, 2008, viewed 8 November 2010, http://www.austlii.edu.au/au/other/alrc/publications/reports/108/
36. Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 18.
37. ALRC submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 2. See also ALRC, *For your information: Australian privacy law and practice*, Report 108, 2008 where the Commission recommended that the TIA Act should be amended to provide for reporting requirements relating to the use of stored communication warrants equivalent to the interception warrant reporting requirements under Part 2-7 and section 102 of the TIA Act (recommendation 73-4).
38. Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 19.

Schedule 5 — Notifying Managing Directors of warrants

This Schedule will amend several notification provisions in the TIA Act to allow notifications to be made to a carrier representative authorised by the Managing Director. Currently, notifications can be made only to a carrier's Managing Director.

Item 1 inserts a definition of 'authorised representative' in the TIA Act. The definition will include the Managing Director and the secretary of the carrier, and also, an employee authorised by either of these people.

Items 2 to 36 makes minor amendments to various provisions relating to warrants consequent on the proposed new definition of 'authorised representative'.

Item 38 provides that the Schedule will apply to warrants issued before its commencement where a notification referred to in one of the proposed amended provisions has not been revoked.

Schedule 6 — Cooperation and assistance function for intelligence agencies

This Schedule proposes amendments to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act) to enable ASIO, ASIS, DSD and DIGO to cooperate more closely and to assist in the performance of one another's functions. The four organisations will also be able to assist other agencies prescribed by Regulation.

The Schedule will also amend the communications provisions in the ASIO Act to remove barriers and to enhance intelligence sharing amongst the national security community.

Amendments to ASIO Act

Items 1 to 6 insert proposed new definitions in section 4 of the ASIO Act that will be consistent with similar definitions in the IS Act.

Item 7 inserts a definition of 'law enforcement agency'. The definition is necessary because of **proposed section 19A** (item 17), which will permit ASIO to cooperate with and provide assistance to law enforcement agencies.

Item 8 inserts in section 4 a definition of 'serious crime' for the purposes of **proposed subsection 18(3)** (item 12). The definition includes conduct that 'if engaged in within, or in connection with, Australia, would be an offence against Commonwealth, State or Territory law punishable by over 12 months imprisonment'.

The Explanatory Memorandum explains that the term 'serious crime' will replace the term 'indictable offence', which can have slightly different meanings in different jurisdictions, and that it will be consistent with the definition of 'serious crime' in the IS Act.[39]

Item 9 inserts a definition of 'staff member'. The definition is intended to include agencies, departments, police and statutory office holders and persons employed or working for those bodies regardless of the way they are engaged.[40]

Section 17 sets out ASIO's functions. These include 'the communication of information relevant to security 'for purposes relevant to security and not otherwise'. **Item 10** removes the words 'and not otherwise' from paragraph 17(1)(b). The Attorney-General's Department has explained that:

> This removes ambiguity that could arise if another provision were to purport to authorise ASIO to communicate security information for purposes other than security, but not specifically state that it overrides the 'and not otherwise' limitation.[41]

Item 11 inserts **proposed paragraph 17(1)(f)** which will enable ASIO to assist bodies referred to in **proposed section 19A** (item 17) in accordance with that section.

Item 12 repeals subsection 18(3) and replaces it with **proposed subsections (3), (4), (4A) and (4B)**. Section 18 relates to the communication of intelligence on behalf of ASIO by the Director-General or by a person authorised by the Director-General.

Proposed subsection (3) will allow information to be transmitted to a Minister, staff member of a Commonwealth or a State authority (**specified in proposed subsection (4)**) by ASIO where:

- the information has come into ASIO's possession in the course of performing the agency's functions under section 17 of the ASIO Act ( ); and
- the information relates or appears to relate to the commission, or intended commission, of a serious crime; or
- the Director-General or the authorised person is satisfied that the national interest requires the communication.

The information must relate to, or appear to relate to the functions, responsibilities or duties of a person specified in **proposed subsection 18(4)** (**proposed paragraph 18(3)(c)**).[42]

---

39. Ibid., p. 24.
40. Ibid., p. 25.
41. Attorney-General's Department submission to Senate Legal and Constitutional Affairs Committee inquiry, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 3, viewed 4 November 2010, http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommuinication_interception_intelligence_services_43/submissions.htm
42. 'Authority of the Commonwealth' is defined in section 4 of the ASIO Act. Amongst other things it includes a Department of State or an Agency within the meaning of the *Public Service Act 1999.*

Proposed subsection 18(4A) will make similar provision for the transfer of information by ASIO to ASIS, DSD or DIGO.

Proposed subsection 18(4B) provides for the communication of information in accordance with an emergency declaration under Part V1A of the Privacy Act. It replicates the substance of current paragraph 18(3)(c).

The Law Council of Australia (Council) queries the meaning of 'national interest',[43] noting that the proposed amendment would let ASIO share information with government agencies:

> ... even where the information does not relate to the commission or planned commission of an offence either within Australia or abroad.[44]

The Council also queries how use of the discretion would be monitored, including whether ASIO will be required to report periodically to the Minister and the public about its exercise of the proposed power.[45]

The Castan Centre comments that presently under the ASIO Act, the information would have been obtained overseas or concern matters outside Australia, thereby tending to confine the notion to traditional foreign policy concerns. However, the proposed amendments would invite a much broader construction.[46]

In response to these concerns, ASIO has said that decisions as to what is and is not in the national interest:

> ... are serious decisions made at the most senior levels of ASIO.... judgements which have always been made by the Director-General of Security.

The agency also sought to disabuse the Senate Legal and Constitutional Affairs Committee of any impressions that ASIO was:

> ... now going to have a spin-offline of business that with every warrant we have we must produce something for other agencies.[47]

Item 14 makes a consequential amendment to section 19 of the ASIO Act under which ASIO may cooperate with certain authorities to the extent necessary or conducive to the performance of its functions. The **proposed amendment** will seek to clarify that the cooperation provided for under **proposed subsection 19(1)** will be confined to the performance of ASIO's functions and not those of the authorities with whom ASIO is cooperating.

---

43. The Australian Privacy Foundation also considers this test too wide: see the Foundation's submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 4.
44. Law Council of Australia submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p.3.
45. Ibid.
46. Castan Centre submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p.4.
47. D Fricker, Deputy Director-General, Australian Intelligence and Security Organisation, evidence before Senate Legal and Constitutional Affairs Committee inquiry into the Bill, op. cit., p. 25.

Item 17 inserts **proposed subsection 19A(1)** to enable ASIO to cooperate with and assist ASIS, DSD, DIGO, a law enforcement agency, or prescribed Commonwealth or State authorities in the performance of their functions. **Proposed subsection 19A(2)** makes this subject to:

> ... any arrangements made or directions given by the Minister; and
> at the request of the head of one of the agencies described in subsection (1).

The Explanatory Memorandum says that, subject to these limits, the decision to provide cooperation or assistance will be a discretionary matter for ASIO, and that agency heads 'may make arrangements concerning the details and/or restrictions on particular instances of cooperation or assistance'.[48]

The Explanatory Memorandum also states that in:

> ... carrying out the proposed new function of cooperating with and assisting other agencies, ASIO must still adhere to the requirements of the ASIO Act.[49]

The Castan Centre expresses concern at the combined effect of the amendments proposed by items 10, 11 and 17, challenging the assertion made in the Explanatory Memorandum that that the Bill 'does not affect the distinction between law enforcement and intelligence functions'.[50] The Centre notes:

> [t]he concerns of ASIO are necessarily very different from those of a police force or a public prosecution service.[51]

The Law Council also queries how:

> ... the distinction between law enforcement and intelligence functions can be guaranteed if proposed section 19A does not require any nexus between the type of work that ASIO may do for other agencies and ASIO's existing functions.[52]

Amendments to IS Act

Items 18 and 19 propose the exclusion of information obtained solely under proposed paragraph 6(1)(da) from the definitions of 'incidentally obtained intelligence' and 'intelligence information' in section 3 of the IS Act. The Explanatory Memorandum states that information falling within these

48. Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 28.
49. Ibid.
50. Castan Centre, op. cit., p. 5, quoting excerpt from Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 1.
51. Ibid.
52. Law Council of Australia submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 4.
52. Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 5.

definitions would have to be communicated in accordance with subsection 11(2AA)[53] of the IS Act and the Privacy Rules issued by the Minister for Foreign Affairs and Trade under section 15 of the IS Act.[54] The Memorandum says that information obtained under **proposed section 13A** (item 27) needs to be excluded from the application of the Rules:

> ... to ensure that the other provisions of the IS Act do not lead to the situation where information could be collected for the sole purpose of assisting another agency but could not be communicated to that agency.[55]

The Memorandum explains the proposed new cooperation functions of DIGO and DSD do not need to be specifically excluded as they will not be captured by the definition.[56]

Items 20, 21 and 22 insert **proposed paragraphs 6(1)(da) and 6B(f) and 7(f)** to enable ASIS DIGO and DSD to cooperate with and assist other agencies in the performance of their functions. The new functions should be read in conjunction with **proposed section 13A**.

Items 23, 24 and 25 propose amendments to paragraphs 11(2)(d), (e) and (f) to ensure that ASIS, DIGO and DSD are not prevented from performing their new functions (see items 20, 21, 22 and 27). Subsection 11(2) places limits on the functions of ASIS, DIGO and DSD in relation to Police functions or any other law enforcement function.

Subsection 11(1) provides that the functions of the three agencies are only to be performed 'in the interests of Australia's national security, Australia's foreign relations or Australia's economic well-being, and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia'.

The Explanatory Memorandum states that:

> The proposed new cooperation and assistance functions are intended to enable the agencies to assist other agencies in the performance of the other agencies' functions, which may not be limited to the matters specified in subsection 11(1).[57]

Item 26 proposes amendments to subsection 11(3) to provide that the limitations on the functions

---

53. The subsection provides for the communication of incidentally obtained intelligence to appropriate Commonwealth/State/approved foreign authorities if the intelligence relates to the involvement, or likely involvement, by a person in: activities that present a significant risk to a person's safety; acting for, or on behalf of, a foreign power; activities that are a threat to security; activities related to the proliferation of weapons of mass destruction or the movement of goods listed in the Defence and Strategic Goods List; committing a serious crime.
54. See http://www.asis.gov.au/privacygov.html, viewed 10 November 2010.
55. Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 28.
56. Ibid., pp. 28, 29.
57. Ibid.

of ASIS, DSD and DIGO do not apply to the proposed new functions of these agencies under items 20, 21 and 22.[58]

Item 27 inserts **proposed new section 13A**. It is framed in similar terms to **proposed section 13A** (item 17).

In view of the fact that the intelligence agencies referred to in the Bill and the information flows between those agencies and other Commonwealth law enforcement agencies under **the proposed regime** will fall outside the ambit of the Privacy Act, the APC recommends that:

> ...an appropriate framework be put in place to support the information sharing arrangements set out in Schedule 6...[59]

In response, the Attorney-General's Department has pointed to the publicly available privacy guidelines to which ASIO and the other agencies are already subject,[60] noting that:

> ... they will need to be reviewed in light of this legislation...[61]

and that the guidelines:

> ... do include guidance as to how ASIO should performance work and include thinks like undertaking inquiries using as little intrusion into individual privacy as possible and using the least intrusive techniques of information collection before more intrusive things.[62]

The Department has also drawn attention to the role of the Inspector-General of Intelligence and Security 'in looking to not only the legality but also the propriety of what ASIO does'.[63]

Amendments to TIA Act

Item 28 makes consequential amendments to subsections 65(1) and 137(1).

Item 29 provides that the amendments in the Schedule relating to the communication of information by ASIO apply to any information whether it comes into ASIO's possession before or after the commencement of the Schedule. The Explanatory Memorandum says that this will ensure:

---

58. Subsection 11(1) of the IS Act provides that the functions of the agencies are to be performed only in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.
59. APC submission to Senate Legal and Constitutional Affairs Committee inquiry into the Bill, p. 15.
60. G McDonald, Deputy Secretary, Attorney-General's Department, evidence before Senate Legal and Constitutional Affairs Committee inquiry into the Bill, Proof Committee Hansard, 11 November 2010, p. 22.
61. Ibid.
62. A Willing, Assistant Secretary, ibid.
63. Ibid.

> ... that these provisions apply to existing information held by ASIO, and that ASIO is not restricted to communicating information only obtained upon commencement of these provisions.[64]

Schedule 7 — Amendments to section 5 of the *Telecommunications (Interception and Access) Act 1979*

Items 1 to 8 of the Schedule propose a number of minor amendments to definitions in subsection 5(1) of the TIA Act, to rectify minor errors and to modernise drafting.

Concluding comments

The Bill is likely to achieve its main objective of facilitating increased cooperation, assistance and information sharing in areas of key national security between ASIO, ASIS, DSD and DIGO and key law enforcement agencies.

This objective will be achieved in large part through the increased sharing of information between the relevant agencies. Particular care will be needed therefore, to ensure an appropriate balance between this and the protection of personal information.

It would seem critical to achieving this balance that:

- appropriate thresholds are provided in the Bill for the collection and use of information; and
- a robust information management system, consistent with Privacy Act principles, is in place from the Bill's commencement date.

Provision in the Bill for the review, after a period of operation, of the Bill's information collection and sharing provisions, including those relating to missing persons, would be highly desirable.

The issues raised by carriers in relation to the proposed Schedule 2 amendments also suggest:

- that the cost and practical efficacy of the proposed new disclosure regime should be carefully monitored; and

- that a review of these amendments would be desirable after a period of operation.

64. Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010, p. 31.

Members, Senators and Parliamentary staff can obtain further information from the Parliamentary Library on (02) 6277 2795.