Law Council
OF AUSTRALIA

Supplementary Information

Telecommunications (Information and Access) Amendment Bill 2008

Senate Legal and Constitutional Affairs Committee

24 April 2008

The Law Council of Australia ("Law Council") is grateful for the invitation to provide supplementary information and respond to the questions taken on notice at the Senate Legal and Constitutional Affairs Committee ("the Committee") hearing into the *Telecommunications (Interception and Access) Amendment Bill 2008* ("the Bill") on 17 April 2008.

NETWORK PROTECTION PROVISIONS

The Law Council was asked in the course of the hearing about its position on extending the sunset clause relating to network protection exemptions.[1]

As explained to the Committee at the hearing, the Law Council does not object to the extension in principle, to the extent that it is designed to allow for a more permanent solution to be put in place.

However, the Law Council endorses the view advanced by the Office of Privacy Commissioner in its written submission to the Committee:

> *The Office supports the position of the Blunn Review that network protection provisions should be accompanied by appropriate privacy protections. Further, in the view of the Office, the subsequent widening of the scope of the network protection exemption to over 20 agencies makes it more important that the safeguards recommended by the Blunn Review are built-into the legislation, including for the purposes of the proposed 18 month extension to the sunset provisions.*
>
> *The Office recommends that consideration be given to amending the TIA Bill to contain more rigorous parameters around the network protection provisions including:*
>
> *a) a prohibition on secondary use of any data accessed for the purpose of protecting the agency's network security, unless there are cogent public policy reasons which reflect community expectations;*
>
> *b) that agencies must clearly identify the people who are given the authorisation under the exemptions; and*
>
> *c) that any data obtained for the purpose of network security should be immediately destroyed when it is no longer needed for that purpose.*

---

[1] During the Inquiry, the Law Council was asked:
Acting Chair: *"Do you have a response to the 18-month extension?" (p. 12)*
Senator Kirk: *"… The sunset clause is being extended for 18 months in order to allow a more comprehensive review to undertaken as to how these matters ought to be dealt with. Has the Law Council given any consideration to the broad question of the Blunn report and a long-term solution to dealing with these matters?" (p. 13)*

CHANGES TO REPORTING OBLIGATIONS

Removal of certain reporting requirements for State interception agencies

During the hearing the Law Council took the following question from Senator Brown on notice:

> *The concern that state agencies may be seeking warrants without the knowledge of their ministers apparently arises out of the legislation as it currently stands. The federal Attorney-General would know but not necessarily the state minister. (p. 14)*

The proposed amendments to section 35 remove the requirement for the chief officer of a State interception agency[2] to provide the responsible Minister in that State with a copy of each warrant issued to the agency and of each instrument revoking such a warrant. The requirement for the responsible State Minister to forward this information to the Commonwealth Minster is also removed by the proposed amendments.

Given all interception agencies are already required to provide copies of every warrant and instrument of revocation to the Secretary of the Attorney-General's Department (AGD), the removal of this requirement is said to be necessary to avoid duplication.

The inclusion of a new section 36 in the 2008 Bill makes it clear, however, that the proposed changes to section 35 do not preclude State Governments from making a law requiring the chief officer of a State interception agency to provide a specified Minister in that State with a copy of each warrant issued to the agency and a copy of each instrument revoking such a warrant.

Privacy Victoria and the Australian Privacy Foundation have expressed concerns regarding the removal of the mandatory requirement for State interception agencies provide copies of warrants to the relevant State Minister. It was submitted that keeping State Ministers informed of warrants issued to State interception agencies was a useful safeguard. Concern was raised that if, as a result of the enactment of the 2008 amendments, the States are required to pass specific legislation requiring States Minsters to be provided with copies of warrants, there is a risk that they will not make the effort and the extra accountability of State Ministers receiving such warrants will be quietly lost.

In response to these concerns, the AGD submitted that other more effective mechanisms already exist to ensure accountability of interception agencies at the State level. In the course of oral submissions, the AGD pointed that, despite the proposed amendments to section 35, reporting requirements will remain that require State interception agencies to report to their responsible State Minster. It was said that these reporting requirements, which require an analysis of the use made of the warrant and the information obtained thereunder, constitute a more meaningful accountability

---

[2] State interception agency (or eligible agency in a State) means: the Police Force of that State; or in the case of New South Wales - the Crime Commission, the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the Police Integrity Commission or the Inspector of the Police Integrity Commission; or in the case of Victoria - the Office of Police Integrity; or in the case of Queensland--the Crime and Misconduct Commission; or in the case of Western Australia - the Corruption and Crime Commission or the Parliamentary Inspector of the Corruption and Crime Commission. *See section 5 of the Telecommunications (Interception and Access) Act 1979 (Cth).*

mechanism than State Ministers receiving a copy of a warrant in bundle of others, which is then passed on to a Commonwealth Minister.

The Law Council also notes that the periodic reports prepared by the AGD and provided to Parliament include statistics on the use of interception warrants by each State interception agency.

Having considered the AGD's submission, the Law Council does not object to the proposed amendment to section 35. As noted in the Blunn Report, if the sole purpose of the State Minsters receiving copies of warrants it to pass them onto the AGD, the existing provisions have been correctly identified as obsolete:

> *Whatever else may be said about this elaborate reporting structure it is difficult to see any useful purpose being served by requiring the State Minister to act merely as conduit.* [3]

It is clear from the proposed section 36 that States will be able to legislate to specifically require State Minsters to receive copies of warrants, without offending against the TIA Act. This would enable States with different standards of accountability or different evaluation frameworks, such as those States with a Charter of Human Rights, to ensure State Ministers have immediate access to copies of all interception warrants.

The Law Council also notes that the AGD has confirmed that the Department has "consult[ed] with the States and the officers of the State ministers on this issue".[4]

POSSIBLE REDRAFTING OF PROVISIONS

The Law Council, in its written submission to the Committee and in oral evidence, stated that it does not object *per se* to more than one telecommunications device being included in a single warrant. The Law Council's objection is to the addition of devices to the warrant after its issue and without the express authorisation of the issuing authority.

The Law Council was asked by the Acting Chair of the Committee to consider how the current provisions of the *Telecommunications (Interception and Access) Act* might be redrafted to allow for a single warrant to authorise interception of communications made by means of more than one device, without diminishing the current safeguards in the warrant regime.

The Law Council has marked up the relevant sections of the *Telecommunications (Interception and Access) Act* to indicate the way that this might be achieved with the most minimal changes.

The Law Council regrets that, within the timeframe allowed by the Inquiry, it has not been able to offer a more comprehensive possible redrafting of the relevant sections.

Likewise, the Law Council has not proposed the introduction of a new procedure whereby an agency may return to the issuing authority to request the addition of a device to the original warrant.

---

[3] Anthony Blunn AO, *Report of the Review of the Regulatoin of Access to Communications,* (August 2005) at [8.17].

[4] See Ms Smith's answer to a question from Senator Hogg p. 38

s9A Issue of named person warrants by Attorney-General

(1) Upon receiving a request by the Director-General of Security for the issue of a warrant under this section in respect of a person, the Attorney-General may, under his or her hand, issue a warrant in respect of the person if the Attorney-General is satisfied that:

(a) the person is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, activities prejudicial to security; and

(b) the interception by the Organisation of:

(i) communications made to or from telecommunications services used by the person; or
*(ii) communications made by means of **any telecommunications device or devices used by the person and identified in the warrant request**;*

will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relating to security; and

(c) relying on a telecommunications service warrant to obtain the intelligence would be ineffective.

(1A) The warrant authorises persons approved under section 12 in respect of the warrant to intercept, subject to any conditions or restrictions that are specified in the warrant:

(a) communications that are being made to or from any telecommunications service that the person is using, or is likely to use; or
*(b) communications that are being made by means of **any telecommunications device or devices identified in the warrant.***

*Note: Subsection (3) restricts the issuing of a warrant authorising interception of communications made by means of **telecommunications devices identified in the warrant.***

(1B) The warrant may authorise entry on any premises specified in the warrant for the purpose of installing, maintaining, using or recovering any equipment used to intercept such communications.

(1C) The reference in paragraph (1)(b) to the interception of communications made to or from a telecommunications service includes a reference to the accessing of the communications as stored communications after they have ceased to pass over a telecommunications system.

(2) A request by the Director-General of Security for the issue of a warrant in respect of a person:

(a) must include the name or names by which the person is known; and
(b) must include details (to the extent these are known to the Director-General of Security) sufficient to identify the telecommunications services the person is using, or is likely to use; and
*(ba) **if the warrant would authorise interception of communications made by means of one or more telecommunications devices identified in the warrant - must include details sufficient to identify each particular telecommunications device that the person is using, or is likely to use**; and*
(c) must specify the facts and other grounds on which the Director-General of Security considers it necessary that the warrant should be issued, including the grounds on

which the Director-General of Security suspects the person of being engaged in, or of being likely to engage in, activities prejudicial to security.

*(3) The Attorney-General must not issue a warrant that authorises interception of communications made by means of **any telecommunications device or devices identified in the warrant** unless he or she is satisfied that:*

(a) there are no other practicable methods available to the Organisation at the time of making the application to identify the telecommunications services used, or likely to be used, by the person in respect of whom the warrant would be issued; or
(b) interception of communications made to or from a telecommunications service used, or likely to be used, by that person would not otherwise be practicable.

Like amendments would be required to section 11B which is drafted in similar terms to 9A and deals with named person warrants issued to ASIO for the collection of foreign intelligence.

Section 46A Issue of named person warrant by a Judge or AAT Member

(1) Where an agency applies to an eligible Judge or nominated AAT member for a warrant in respect of a person and the Judge or nominated AAT member is satisfied, on the basis of the information given to the Judge or nominated AAT member under this Part in connection with the application, that:

(a) Division 3 has been complied with in relation to the application; and
(b) in the case of a telephone application--because of urgent circumstances, it was necessary to make the application by telephone; and
(c) there are reasonable grounds for suspecting that a particular person is using, or is likely to use, more than one telecommunications service; and
(d) information that would be likely to be obtained by intercepting under a warrant:
(i) communications made to or from any telecommunications service that the person is using, or is likely to use; or
*(ii) communications made by means of **any telecommunications device or devices used by the person and identified in the warrant application**;*

would be likely to assist in connection with the investigation by the agency of a serious offence, or serious offences, in which the person is involved; and

(e) having regard to the matters referred to in subsection (2), and to no other matters, the Judge or nominated AAT member should issue a warrant authorising such communications to be intercepted;

the Judge or nominated AAT member may, in his or her discretion, issue such a warrant.

*Note: Subsection (3) restricts the issuing of a warrant authorising interception of communications made by means of **telecommunications devices identified in the warrant**.*

(2) The matters to which the Judge or nominated AAT member must have regard are:

(a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant:

(i) communications made to or from any telecommunications service used, or likely to be used, by the person in respect of whom the warrant is sought; or
*(ii) communications made by means **any telecommunications devices identified in the warrant and used, or likely to be used, by the person in respect of whom the warrant is sought;***

as the case requires; and

(b) the gravity of the conduct constituting the offence or offences being investigated; and
(c) how much the information referred to in paragraph (1)(d) would be likely to assist in connection with the investigation by the agency of the offence or offences; and
(d) to what extent methods (including the use of a warrant issued under section 46) of investigating the offence or offences that do not involve the use of a warrant issued under this section in relation to the person have been used by, or are available to, the agency; and
(e) how much the use of such methods would be likely to assist in connection with the investigation by the agency of the offence or offences; and
(f) how much the use of such methods would be likely to prejudice the investigation by the agency of the offence or offences, whether because of delay or for any other reason.

*(3) The Judge or nominated AAT member must not issue a warrant that authorises interception of communications made by means of **any telecommunications device identified in the warrant** unless he or she is satisfied that:*

(a) there are no other practicable methods available to the agency at the time of making the application to identify the telecommunications services used, or likely to be used, by the person in respect of whom the warrant would be issued; or
(b) interception of communications made to or from a telecommunications service used, or likely to be used, by that person would not otherwise be practicable.

Subsection 42(4A): Information to be included in an affidavit accompanying an application for a named person warrant

(4A) If the application is for a named person warrant, the affidavit must set out:

(a) the name or names by which the person is known; and
(b) details (to the extent these are known to the chief officer) sufficient to identify the telecommunications services the person is using, or is likely to use; and
*(ba) **if the warrant would authorise interception of communications made by means of one or more telecommunications device or devices identified in the warrant– details sufficient to identify each telecommunications device the person is using, or is likely to use;** and*
(c) the number of previous applications (if any) for warrants that the agency has made and that related to the person or to a service that the person has used; and
(d) the number of warrants (if any) previously issued on such applications; and
(e) particulars of the use made by the agency of information obtained by interceptions under such warrants.

Sections 16(1A) and 60(4A) of the TIA Act should be repealed.

These subsections set out the procedure for notifying a telecommunications carrier of the intention to intercept telecommunications made by means of a telecommunications device *not named in the warrant.*

These subsections therefore serve no purpose.

Attachment A

Profile – Law Council of Australia

The Law Council of Australia is the peak national representative body of the Australian legal profession. The Law Council was established in 1933. It is the federal organisation representing approximately 50,000 Australian lawyers, through their representative bar associations and law societies (the "constituent bodies" of the Law Council).

The constituent bodies of the Law Council are, in alphabetical order:

- Australian Capital Territory Bar Association
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society of the Australian Capital Territory
- Law Society of the Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar Association
- The Victorian Bar Inc
- Western Australian Bar Association
- LLFG Limited (a corporation with large law firm members)

The Law Council speaks for the Australian legal profession on the legal aspects of national and international issues, on federal law and on the operation of federal courts and tribunals. It works for the improvement of the law and of the administration of justice.

The Law Council is the most inclusive, on both geographical and professional bases, of all Australian legal professional organisations.