Australian Government

Attorney-General's Department

Security and Critical
Infrastructure Division

08/6895

8 April 2008

Secretary
Senate Legal and Constitutional Affairs Committee
Department of the Senate
Parliament House
Canberra ACT 2600

Email:legcon.sen@aph.gov.au

Dear Secretary

Submission to the Senate Standing Committee on Legal and Constitutional Affairs inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008

I am pleased to provide the Attorney-General's Department submission to the Committee's inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008 (the Bill).

The Bill amends the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to extend the operation of the existing sunset provisions. This is to enable the development of a full legislative solution that clarifies the basis upon which specified network administrators may access communications within their network for the purposes of network security and the enforcement of professional integrity.

The Bill also amends the TIA Act to improve the effectiveness of the telecommunications access regime by:

- clarifying that multiple telecommunications devices can be intercepted on the one named person warrant
- amending and clarifying agencies' reporting requirements under the TIA Act, and
- making minor and technical amendments arising from the transfer of duties from the Australian Federal Police (AFP) to the Attorney-General's Department following the passage of the *Telecommunications (Interception) Amendment Act 2006*.

Extension of sunset provisions

Networks are protected from security risks by the use of gateway control systems. The use of these systems (such as virus protection software) does not generally contravene interception legislation. Automated systems can screen and reject incoming communications if they are suspected of containing a virus, and network operators are able to monitor internal and outbound communications (including emails and internet browsing) provided they have obtained the consent of people using the network. However, some network protection activities that take place at the threshold of a network may constitute a technical breach of the TIA Act.

The network protection provisions initially applied to the Australian Federal Police and were inserted by the *Telecommunications (Interception) Amendment Act 2006*. These provisions were subject to two-year sunset clauses that come into effect on 13 June this year. They were extended to the wider group of agencies by the *Telecommunications (Interception and Access) Amendment Act 2007*, but the original sunset clauses were retained.

To enable the continued protection of specified secure networks, the Bill extends the sunset provisions by 18 months so that specified agencies will continue to be allowed to monitor all communications within their corporate networks for the purposes of protecting and maintaining their networks and enforcing professional standards. The specified agencies encompass criminal law enforcement agencies that may access telecommunications interception, as well as defence and intelligence agencies.

While significant progress has been made by the Department towards a full legislative solution, the additional 18 months will allow adequate time to finalise the policy development and undertake consultation with state and territory governments and a broad range of non-government stakeholders. The additional 18 months will also allow for any issues raised during these consultations to be fully considered and incorporated where appropriate.

Device-based named person warrants

Named person warrants were introduced in 2000 to reflect the advances in technology which targets had taken advantage of with the express purpose of avoiding law enforcement detection, such as the use of multiple telecommunications services. The increase in the availability of low cost handsets since this time provides further opportunities for targets to avoid investigation by law enforcement agencies. Sophistication in criminal groups and organised crime together with technological advancements has increased the complexity of methods used to avoid detection.

The *Telecommunications (Interception) Amendment Act 2006* distinguished between telecommunications services and telecommunications devices to reflect the increase in the number of telecommunications devices being used again by targets to avoid detection.

The TIA Act provides for the issue of a named person warrant, which can be based on either the services (such as the SIM card or e-mail account) or the devices (such as a mobile handset or personal computer) being used by a target to communicate. The main difference is that device-based interception enables the interception of multiple services via an identified communications device without the need to identify individual services being operated by that device.

A service-based named person warrant authorises the interception of 'any telecommunications service' that the target is using and allows the addition of telecommunications services to the named person warrant as they are identified (subparagraph 9A(1)(b)(i) and subsection 16(1)). However, the provisions for a device-based named person warrant are inconsistent in that they permit the notification of additional devices to a warrant after it has been issued (subsections 16(1A) and 60(4A)), but only authorise interception by means of a 'particular device' (subparagraphs 9A(1)(b)(ii) and 46A(1)(d)(ii)) rendering the former provisions inoperable.

The Bill clarifies the legislative intention of the *Telecommunications (Interception) Amendment Act 2006* that introduced the concept of device-based named person warrants to allow multiple devices to be intercepted in connection with one named person warrant, and allow additional devices to be added to that warrant if and when they are identified by the relevant agency.

The primary issue of the interference with person's privacy is addressed by the issuing authority in considering whether to grant a device-based named person warrant. The interception agency must satisfy the issuing authority that:

- there are no other practicable methods available at that time to identify the telecommunications services being used, or likely to be used, by the person of interest, or
- it is impracticable to intercept the service being used by the person of interest.

Once, this threshold is met, a device-based named person warrant is then intended to permit interception of any of the target's communication devices once identified.

Device-based interception is also subject to the existing privacy protections in the interception regime, including the following factors to be considered by an issuing authority before granting an interception warrant:

- the impact the interception will have on the privacy of any persons as a result of intercepting communications made from any service or of a particular device used or likely to be used by the person of interest
- the extent to which alternative methods of investigation have been used by the interception agency, and
- that the interception is for an investigation of a serious offence, generally punishable by a maximum period of imprisonment of at least seven years.

The reference to 'particular device' is a reference to being able to identify that a particular device is connected to a particular person. Unlike a telecommunications service that has an inherently unique identifier, such as the telephone number or email address, telecommunications devices are uniquely identified by other means.

All telecommunications devices, such as a mobile handset or a laptop computer, have a unique identifier that allows the device to interact with telecommunications networks. For example, the unique identifier for a mobile handset is called an International Mobile Equipment Identifier (IMEI). A unique identifier for a computer or any wireless connected device is a Media Access Control (MAC) address. It is possible to match the unique identifier of the device to a particular person via subscriber detail or through the monitoring of known telecommunications services that the person of interest is using.

Interception agencies undertake extensive enquiries with carriers to ensure that device-based interception is based on a unique number and the integrity of the regime is preserved. These extensive checks and associated processes are intended to continue where an additional device is identified as being used by the person of interest and intended to be added to an existing device-based named person warrant.

The Bill allows the head of an agency or a senior officer or staff member of an agency who has been approved in writing by the chief officer of an agency, to approve the addition to the warrant of an additional device and to notify the relevant carrier. The senior officer is not able to make decisions that go beyond the limits of the original warrant and therefore is required to be satisfied that the addition of a device to a named person warrant would meet the thresholds that an issuing authority must have regard to, or be satisfied of, in issuing the original warrant.

There are a number of accountability mechanisms in place for interception warrants, including:

- An interception agency is required to revoke a warrant when the grounds for the warrant no longer exist. This includes where it is no longer impracticable to intercept telecommunications services being used by the person.
- Intercepted material must be destroyed where it is not relevant to the permitted purposes of the agency – generally an investigation of an offence that is punishable by three years imprisonment or more.
- An issuing authority may impose conditions or restrictions on an interception warrant.
- The Ombudsman has independent oversight of the conduct of the interception agencies in carrying out interception.

Reporting requirements

The Bill amends agencies reporting requirements under the TIA Act in relation to the notification of interception warrants and instruments of revocation by:

- delegating the notification obligations of a 'chief officer' of an interception agency to a 'certifying officer' of the agency to improve the balance between accountability and operational effectiveness, and
- requiring an agency to notify the Secretary of the Department when an additional service or device is added to a named person warrant to ensure all services and devices intercepted are entered into the General and Special Registers of Warrants.

The Bill also amends incorrect references to a 'certifying person' to a 'certifying officer' in relation to the notification of additional devices being added to a device-based named person warrant.

Transfer of duties

The *Telecommunications (Interception) Amendment Act 2006* repealed the Telecommunications Interception Remote Authority Connection (TIRAC). TIRAC was an accountability mechanism whereby the AFP would receive a lawfully issued interception warrant; would then enable the interception, and subsequently disable the interception when the warrant expired. TIRAC also gave the AFP an oversight role by examining the validity of warrants issued to other agencies.

With the ceasing of TIRAC, the oversight function was transferred to the Department; all of the provisions relating to TIRAC were amended so that an action previously the responsibility of the Commissioner of the AFP was now the responsibility of the Secretary of the Department. These amendments created a significant residual duplication of reporting requirements for warrants issued under Part 2-5 of the TIA Act to the Secretary of the Department. The Bill removes these duplicate reporting requirements and the requirement for an interception agency to undertake cost agreements with the AFP to undertake this function.

Consistent with recommendation 27 of the *Report of the Review of the Regulation of Access to Communications* by Mr Tony Blunn AO (the Blunn Review), the Bill also removes the unnecessary duplicate reporting requirements for a State interception agency to provide copies of their warrants and revocations to a relevant State Minister, who is then required to forward copies of the warrants to the Attorney-General. However, rather than removing the requirement for State Ministers to be given copies of each warrant and revocation, the Bill provides that State legislation may make provision for the relevant State Minister to receive a copy of each warrant and instrument of revocation.

The action officer for this matter is Wendy Kelly who can be contacted on 6250 5403.

Yours sincerely

[redacted]

Jonathan Curtis
A/g Assistant Secretary
Telecommunication and Surveillance Law Branch

Telephone: 6250 6359
Facsimile: 6250 5940
E-mail: jonathan.curtis@ag.gov.au