Law Council
OF AUSTRALIA

Inquiry into the *Telecommunications (Interception and Access) Amendment Bill 2008*

Senate Legal and Constitutional Affairs Committee

4 April 2008

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

Law Council of Australia Limited
ABN 85 005 260 622
www.lawcouncil.asn.au

Introduction

On 20 February 2008, Attorney-General Robert McClelland introduced the *Telecommunications (Interception and Access) Amendment Bill 2008* into Parliament. The Bill was considered time-critical due to the expiry of a sunset clause in section 5F of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

At the time the 2008 Bill was introduced, the Law Council raised a number of concerns with Parliamentarians and the Attorney-General's Department. The Law Council now welcomes the opportunity to provide a submission to the Senate Legal and Constitutional Affairs Committees' Inquiry into the Bill.

The 2008 Bill:

- extends (by 18 months) the sunset clause for network protection provisions that create exemptions to the general prohibition on listening to or copying communications passing over the telecommunication system;
- amends provisions relating to reporting obligations to avoid duplication; and
- extends the existing device-based named person warrant regime to authorise the interception of communications made by multiple telecommunications devices.

In his Second Reading speech introducing the 2008 Bill, Attorney General Robert McClelland states that the Bill:

> *"… contains no new powers for security or law enforcement agencies in relation to telecommunications interception, stored communications or access to data, but the bill ensures that these agencies have the necessary tools to combat crime in this age of rapid technological change."*

The Law Council does not believe that this is entirely accurate.

On the contrary, the Law Council believes that, if passed, the proposed amendments relating to device-based named person warrants will result in yet another incremental expansion in the telecommunication interception powers of ASIO and law enforcement agencies.

The Law Council recommends that the proposed amendments be modified to ensure that:

- while a single warrant may authorise interception of telecommunications made by means of multiple devices, each of those devices must be named in the warrant; and

- the issuer of the warrant must be satisfied that:

    - the person named in the warrant is using or is likely to use each device from which communications will be intercepted;

    - each of the devices used or likely to be used by the named person can be uniquely and reliably identified for interception purposes; and

    - the communications likely to be made by means of each device from which communications will be intercepted are likely to yield information useful to the investigation.

Law Council concerns with proposed amendments to device based named person warrants

Authorising interception from multiple telecommunications devices

The proposed amendments seek to allow ASIO and law enforcement officers to obtain a blanket authorisation to intercept all communications made by means of *any telecommunications device* used by a named person of interest. The amendments will dispense with the current requirement that in order to obtain a device-based interception warrant, the officer seeking the warrant[1] must first identify the *particular* telecommunication device in relation to which they hope to intercept all communications.

This is of concern to the Law Council because it equates to a further loosening of the telecommunications interception warrant regime.

The Law Council believes that in order to obtain a telecommunications interception warrant it should not be enough that ASIO or law enforcement agencies satisfy the issuer of the warrant:[2]

- that the person whose telecommunications they seek to intercept is a legitimate target of suspicion from a security or law enforcement perspective; and

- that intercepting that person's telecommunications is likely to yield useful information for the investigation which could not be obtained by other means.

The Law Council believes that ASIO and law enforcement agencies should also be required to satisfy the issuer of the warrant, on the basis of available evidence, that:

- each and every telecommunications service or telecommunications device that they seek authorisation to intercept is, in fact, used or likely to be used by the relevant person of interest; and

- each and every telecommunications service or telecommunications device that they seek authorisation to intercept can be uniquely identified such that relevant telecommunications made using that service or device can be isolated and intercepted with precision.

Requiring the issuer of the warrant to be satisfied of all these matters recognises that there are a number of ways that telecommunications interception, undertaken for law enforcement or national security reasons, may inadvertently result in the unjustified invasion of a person's privacy. For example:

---

[1] Under section 9A of the TIA Act, the Director-General of Security may request a named person warrant on behalf of ASIO. Under section 46A of the TIA Act, the Australian Federal Police, the Australian Commission for Law Enforcement Integrity or the Australian Crime Commission can apply for a named person warrant. Eligible State agencies may also apply.

[2] Under section 9A of the TIA Act, the Attorney-General, on request from the Director General of Security, can issue a named person warrant to ASIO. Under section 46A of the Act, an eligible Judge or AAT member can issue a named person warrant to an agency (s46A).

1. ASIO or a law enforcement agency may have erroneously identified their suspect, perhaps as a result of acting prematurely or on the basis of unreliable information.

2. ASIO or a law enforcement agency may have misjudged the nature of the communications that the targeted person was likely to engage in using the intercepted service or device and as a result the information obtained may be entirely personal and of no relevance to the investigation.

3. ASIO or a law enforcement agency may have correctly identified their suspect *but* may have erroneously identified the telecommunications services or devices used by that person, (again perhaps on the basis of incomplete or unreliable information), with the result that the communications of an innocent third party are intercepted.

4. ASIO or a law enforcement agency may have correctly identified their suspect and correctly identified the telecommunication service or devices used by that person *but* may not be technically able to uniquely identify telecommunications made using that service or device without the risk of intercepting communications made via an unrelated service or device. (This appears to be more of a real risk with device based, rather than service based, interception as discussed below.)

The proposed amendments will significantly reduce the role of the warrant authorisation process in safeguarding against errors of the kind described in 3 and 4 above.

The amendments will allow a single warrant to be issued which authorises the interception of multiple telecommunications devices used by or likely to be used by a person of interest.

That one warrant might authorise the interception of multiple devices is not in itself objectionable. The problem is that neither the application nor the warrant need exhaustively list all the devices which may be intercepted pursuant to the warrant.

Under the proposed amendments, the officer applying for the warrant must provide details, *to the extent that they are known to him or her* at the time of making the application, sufficient to identify the telecommunications devices used or likely to be used by the named person who is the subject of the warrant. However, if ASIO or a law enforcement agency later forms the view that other devices, not listed in the warrant application, are also being used by or are likely to be used by the named person, then telecommunications made by means of those additional devices may also be intercepted pursuant to the warrant. This may occur, notwithstanding the fact that the issuer of the warrant has given no consideration as to whether there is sufficient available evidence to link the named person to those additional targeted devices or whether there is sufficient available information to uniquely identify those devices for interception purposes.

This is a significant departure from the current provisions governing the issue of device-based named person warrants which require the officer seeking the warrant to provide sufficient details to identify *the particular* device that the person named in the warrant is using or likely to use. Under the current provisions, if a warrant is issued, the particular telecommunications device must be identified in the warrant and only communications made by means of that particular device may be intercepted pursuant to the warrant.

The significance of the proposed amendments has been played down on the basis that they will do no more than bring the provisions governing the issue of device-based

named person warrants into line with the provisions governing the issue of service-based named person warrants. To that end, the amendments have been presented as largely technical in nature.

The fact that ASIO and law enforcement agencies are already able to obtain a blanket authorisation to intercept all communications made to or from *any telecommunications service* used by a named person of interest, without having to exhaustively list those services, dose not assuage the Law Council's concerns.

The Law Council believes that the provisions which govern the issue of service-based named person warrants provide inadequate external oversight and safeguard against the inadvertent interception of the private communications of innocent third parties. No compelling argument has been presented for why these more liberal provisions should become the default standard, to which other warrant regimes are aligned.

Problems with uniquely identifying telecommunication devices

In addition to the concerns outlined above, the Law Council believes that there are good reasons for approaching device-based interception warrants with more caution than service-based warrants.

Device-based named person warrants were inserted into the TIA Act in 2006. The Explanatory Memorandum to the 2006 Bill explained that device based named person warrants were introduced to:

> *assist interception agencies to counter measures undertaken by persons of interest to evade telecommunications interception such as adopting multiple telecommunications services.*
>
> *The amendments will enable interception agencies to apply to an issuing authority for a named person warrant to intercept communications from identified telecommunication devices. An issuing authority must not authorise interception on the basis of the telecommunications device unless satisfied that the applicant agency has not practicable methods of identifying the telecommunications services used or likely to be used by the person of interests, or that interception of those services would not be possible. The latter situation covers instances in which agencies may be able to identify all services, but it is impracticable to intercept each service. For example, a person of interest may transfer hundreds of different Subscriber Identity Module (SIM) cards through a mobile handset in quick succession. Interception of each telecommunications services (currently identified by reference to the SIM card) is extremely impracticable to achieve before the person of interest changes the SIM card being used.*

A "telecommunications device" is defined as "a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system." In the Explanatory Memorandum to the 2006 Bill "terminal devices" were described as "any end piece of telecommunications equipment by which a person may communicate, including a mobile handset, personal computer, or personal digital assistance".

In order to facilitate interception, the device must be capable of being uniquely identified, so that telecommunications made by means of that device can be isolated and intercepted.

For this reason, the 2006 Bill inserted a definition of "telecommunications number" into the TIA Act as a means by which interception agencies may identify the telecommunications device subject to an interception warrant. The Explanatory Memorandum to the 2006 Bill stated:

> *A telecommunications device may be identified by any unique number including a telephone number for mobile phone handsets, a Media Access Control address for computer terminals, or an e-mail address. The definition of telecommunications number is inclusive so as not to limit the unique numbers which may be used to identify telecommunications devices, thereby maintaining a technology neutral approach to the regulation of telecommunications interception.*

However, as noted by the Senate Standing Committee on Legal and Constitutional Affairs in their Inquiry into the 2006 Bill, uniquely identifying telecommunication devices can be problematic, particularly given the unreliable character of existing telecommunication device identification systems. The Senate Committee expressed concern that:

> *It was not clear from the evidence the extent to which [existing device identification processes, such as the use of telephone numbers] would guarantee that the device being targeted under the warrant was able to be certified as uniquely identifiable.*

Similar concerns had been raised in the Blunn Report, where it was recommended that:

> *priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.*

In it's submission to the Senate Inquiry, Electronic Frontiers Australia (EFA) considered it to be "highly inappropriate" to permit equipment-based interception prior to the development of a unique and indelible identifier of the source of telecommunications. The EFA was strongly opposed to named person warrants being issued on the basis of device numbers that may identify multiple items of equipment.

The Senate Committee found that there was "a sound basis" for EFA's concerns. Officers of the Attorney-General's Department acknowledged that there was potential for duplication of numbers thought to be unique, as did the AFP who, in response to questioning about device based named person warrants, stated that there is the possibility that the unique identifying number for a telephone or computer may get mixed up with other telephones or computers:

> *We would make all [the] efforts we could to ascertain that [the unique identifying number] through our inquiries to the telecommunications companies. The concern, of course, is that some of these are fraudulently obtained.*

Reservations were also expressed by the Privacy Commissioner, who provided the following recommendation to the Senate Inquiry:

> *"The Office has not been able to fully determine the limits to the scope of the operation of [the device based named person warrants], and so recommends that careful consideration be given to ensuring that the provisions … do not give rise to unintended reduction of the privacy provisions in the Interception Act."*

The Senate Committee arrived at the view that:

> *any arrangement designed to target a specific piece of equipment should be able to identify it with a high degree of certainty. It is the Committee's view that while there is a clear operational requirement for law enforcement agencies to be able to target specified devices, doubts remain over their capacity to identify these devices with a high degree of certainty.*

The Senate Committee recommended:

> *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.*

In its response to the Senate Committee's report, the Government acknowledged the importance of developing a reliable system of unique identification of telecommunications devices as a basis for access to communications and stated:

> *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.* (Emphasis added)

The proposed amendments appear to constitute a retreat from this position. Far from ensuring *"warrants will only be issued where the requesting agency can show that the unique identifying number is indeed a unique source"*, the proposed amendments will authorise interception of communications from any telecommunications device used by the named person, regardless of whether the device has been referred to at all in the warrant process.

There is no information included in the material supporting the Bill to suggest that the concerns expressed by the Senate Committee in 2006 about the accuracy and reliability of device based interception have been addressed. Nonetheless, the proposed amendments explicitly invite Parliament to treat device-based interception as no more risky or problematic than service based interception.

The Law Council does not purport to hold any expertise in the area of the identification of telecommunication devices. If advances have been made since 2006, then this information should be made available to the Parliament and the public.

The Attorney-General's Department's Responses to the Law Council Concerns

The Law Council's concerns about the proposed changes to the device based name person warrant regime were conveyed to the Attorney-General's Department. The following responses were received:

The Attorney-General's Department claim that the proposed amendments merely clarify the legislative intent of the 2006 amendments

The Attorney General's Department has expressed the view that the 2008 amendments are necessary to clarify the legislative intention at the time of the 2006 Bill "to allow multiple devices to be intercepted in connection with one named person warrant and allow additional devices to be added to a warrant if and when they are identified by the relevant agency."

This intent was said to be evidenced by the inclusion, at the time of the 2006 Bill, of sections 16 and 60(4a) which appear to recognise that named person warrants authorise the interception of multiple devices. The 2008 amendments were therefore necessary because the terminology used when drafting the 2006 legislation has inadvertently rendered these provisions inoperative.

The Law Council disputes the suggestion that the intention of the legislature at the time of the 2006 Bill was to authorise the interception of communications from multiple devices on a single named person warrant.

The Law Council is aware of the contradictions which exist between section 9A and section 16(1A) and between section 46A and 60(4A). The Law Council is also aware of the internal contradictions which exist within section 16 and 60(4A).

The primary sections and which govern the issue of device-based named person warrants, sections 9A and 46A, both clearly state that a device based named person warrant can only be issued in respect of "a particular telecommunications device" and that that device must be "identified in the warrant"

On the other hand, sections 16 and 60(4A), which are merely enabling sections which govern the notification that must be given to telecommunications carriers about the issue of certain warrants, are less clear. As noted, these sections are internally contradictory.

For example, Section 16(1A) provides:

> *16 (1A) Where:*
>
> *(a) the Managing Director of a carrier has been given a copy of a warrant under section 9A or 11B; and*
>
> *(b) **the warrant is a warrant that authorises interception of communications made by means of a telecommunications device identified in the warrant**; and*
>
> *(c) it is proposed, under the warrant, to intercept, by means of a telecommunications device, communications made to or from a telecommunications service operated by the carrier; and*

(d) ***the device was not identified in the warrant****;*

a certifying person must cause the Managing Director of the carrier to be given, as soon as practicable, a description in writing of the device sufficient to identify it.

(Emphasis added)

On the one hand, subsection 16(1A)**(d)** and 60(4A)(**d**) appear to recognise that device-based named person warrants authorise the interception of multiple devices, even where those devices are not identified in the warrant. On the other hand, subsections 16(1A)(**b**) and 60(4A)(**b**) accord with sections 9A and 46A in confirming that the telecommunications device to be intercepted must be identified in the warrant.

In the circumstances, the Law Council cannot accept the assertion that the clear "legislative intention" when the device-based warrants were introduced in 2006 was to allow for warrants which authorised the interception of communications from multiple devices not necessarily identified in the warrant.

On the contrary, the clear legislative intention expressed in the primary provisions governing the issue of device-based named person warrants, namely sections 9A and 46A, was to limit these warrants to authorising the interception of communications from *a particular telecommunications device*.

The Department's assertion about legislative intent is particular unsustainable in light of the response the Government gave at the time to the Senate Legal and Constitutional Affairs Committee which inquired into the provisions of the 2006 Bill. In its written response to the Senate Committee's recommendation concerning device-based named person warrants, the Government stated:

"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" (Emphasis added.)

This undertaking demonstrates a clear legislative intent that the particular device from which communications are to be intercepted would have to be identified at the time the warrant was issued.

The Law Council agrees with Department that Section 16(1A) and section 60(4A) are poorly drafted and need to be revisited.

This should not be used, however, as the pre-text for loosening the regime which governs device-based named person warrants. That regime currently requires the identification of the particular device to be intercepted. It should not be extended to provide the police or ASIO with a blank cheque to intercept any telecommunications device (identified in the warrant or not) which the police or ASIO believe is being used by or might be used by a person of interest.

The Attorney-General's Department's claims that the existing and proposed provisions contain adequate privacy protections

The Department asserts that sufficient privacy protections exist within the named person warrant system. For example:

- Device based interception is only available to interception agencies where they can satisfy an issuing authority that:
    - The applicant agency has exhausted all practical methods of identifying the telecommunications services being used by the person of interest, or
    - It is impractical to intercept the service being used by the person of interest.
- Device based interception is subject to the existing privacy protections in the interception regime, which require the issuing authority to consider the following factors before granting an interception warrant:
    - The impact the interception will have on the privacy of persons using the telecommunications service or device
    - The extent to which alternative methods of investigation have been used by the interception agency, and
    - That it is for the investigation of a serious offence, generally punishable by a maximum period of imprisonment of at least seven years.

The Law Council believes that such privacy protections are of little utility unless the authority issuing the warrant considers each particular device that will be subject to interception.

The issuing authority can not address these privacy tests with appropriate rigour without considering each and every telecommunications device that is to be covered by the warrant. In particular, an issuing authority can not consider "*the impact the interception will have on the privacy of persons using the telecommunications service or device"* if he or she does not even know the telecommunications devices in respect of which the warrant will operate.

Under the 2008 amendments, an issuing authority will not be required to consider whether there is sufficient evidence to establish that the person named in the warrant is using or is likely to use each device from which communications will be intercepted. Nor will he or she be required to consider whether the communications likely to be made by means of each device from which communications will be intercepted are likely to yield information useful to the investigation.

In that context, the issuing authority cannot possibly weigh privacy considerations against asserted operational imperatives.

The Department has stated that:

> *The primary issue of the breach of privacy is addressed by the issuing authority in considering whether to grant a named person warrant.*
>
> *Once this threshold has been met, a device-based named person warrant is then intended to permit interception of any of the target's communication devices.*

The Law Council agrees that the warrant process is the primary means of protecting individual privacy when issuing warrants for telecommunication device interception. However it is difficult to see how the threshold test for privacy can be met where the issuing authority remains unaware of the particular devices to be targeted under the warrant.

For the Law Council, the ability of the warrant system to protect individual privacy depends on the issuing authority considering each individual device from which telecommunications are to be intercepted under the warrant.

The Attorney-General's Department's claims that adequate accountability mechanisms exist under the proposed device based named person warrant regime.

In response to the Law Council's comments on the proposed amendments, the Department listed a number of accountability mechanisms that will exist under the proposed regime. For example:

- An interception agency is required to revoke a warrant when the grounds for the warrant no longer exist.
- Intercepted material must be destroyed where it is not relevant to the permitted purposes of the agency.
- An issuing authority may impose conditions or restrictions on an interception warrant.
- The Ombudsman also has independent oversight of the conduct of the interception agencies in carrying out interception.
- Interception agencies will also be required to notify the Secretary of the Attorney-General's Department of the addition of a device to a device-based named person warrant to enable the compilation of the General and Special Warrant registers which the Attorney-General inspect on a quarterly basis.

All but one of these accountability mechanisms are directed at monitoring the use of interception powers after a warrant has been issued and executed.

The Law Council submits that 'after the fact' reporting or oversight mechanisms are not an adequate substitute for a rigorous, external warrant regime which determines whether, when and how ASIO or police should be exercising interception powers in the first place.

The Attorney-General's Department's claims that it is possible to uniquely identify a telecommunications device

In response to concerns raised by the Law Council about the difficulties associated with accurately and uniquely identifying telecommunications devices, the Attorney-General's Department informed the Law Council that 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 an International Mobile Equipment Identifier (IMEI); a unique identifier for a computer or any wireless connected device is a Media Access Control (MAC address).

According to the Department, it is possible to match the unique identifier of the device to a particular person via subscriber details or through the monitoring of known telecommunications services that the person is using. Interception agencies undertake extensive enquiries with carriers to ensure device based interception is based on a unique number and the integrity of the regime is preserved.

The Law Council emphasises that it has no expertise in the field of telecommunications technology and has limited knowledge of the technology used to identify telecommunications devices. However, the Law Council notes that the 'unique identifiers' referred to and relied upon by the Department (IMEIs and MAC addresses) to unique identify telecommunication devices from which communications were to be intercepted were both discussed at the time the 2006 Bill was introduced. The following extract from report prepared by the Senate Legal and Constitutional Affairs Committee on the Bill reveals that, at that time, there was a risk that such numbers were amendable to duplication:

4.120 In evidence, it became clear that there was a sound basis for EFA's concerns [that unique identifiers are unreliable]. Mr Gifford of the Attorney General's Department acknowledged that there is potential for duplication of numbers thought to be unique:

> *We do understand that risk, and we are aware that there are duplicate IMEIs in a telecommunications network. On that basis, we have said, 'When you're seeking interception on the basis of a handset, it must be defined by reference to a unique telecommunications number, which, for the purposes of the definition, will include an IMEI. … You must satisfy the issuing authority that the IMEI you are seeking interception of is a unique IMEI number.*

4.121 Deputy Commissioner Lawler explained that:

> *… we have seen a practice whereby these numbers have been copied fraudulently within service providers to commit fraud, but also to enable another way of not being able to identify who has the particular handset in question. I understand from the briefings I have received that there is the capacity to remove such duplicate numbers from the system, as there is also the capacity to remove stolen handsets from the system. As has been indicated, we would do the checks that are required for the potential for those numbers to be duplicated on the system, but they are only duplicated through, as I am briefed, a fraudulent activity and the numbers being cloned or copied.*
>
> *In further discussion, the AFP indicated that they would be required to undertake inquiries regarding the uniqueness of the proposed identifier, and to provide details in any application for a warrant the steps which had been undertaken to achieve this.*

If advances have been made since the Senate Committee considered the matter in 2006, the Law Council is of the view that Parliament (and the public) should be appropriately briefed about why device-based interception warrants no longer present the difficulties, challenges and risks that they once did.

It is worth noting again that both the Department and AFP responses to the Senate Committee quoted above indicate that, on their understanding of the relevant provisions, the issuer of the warrant would have to be presented with information about the particular device from which communications would be intercepted. This is contrary to the 'legislative intent' the Department now attributes to the 2006 Bill.

Law Council Recommendations

The Law Council recommends that the proposed amendments be modified to ensure that:

- while a single warrant may authorise interception of telecommunications made by means of multiple devices, each of those devices must be named in the warrant; and

- the issuer of the warrant must be satisfied that:

    - the person named in the warrant is using or is likely to use each device from which communications will be intercepted;

    - each of the devices used or likely to be used by the named person can be uniquely and reliably identified for interception purposes; and

    - the communications likely to be made by means of each device from which communications will be intercepted are likely to yield information useful to the investigation.

Law Council concerns with extending the sunset clauses for network protection exemptions

Subsection 5F(2) and 5G(2) of the TIA Act currently provide Commonwealth agencies[3] with exemptions to the general prohibitions against unauthorised telecommunication interception and access to stored telecommunications.

These exemptions enable Commonwealth agencies to monitor inbound and outbound communications to their network for the purpose of enforcing professional standards and protecting their networks without the risk of breaching the TIA Act.

Sections 5F(2) and 5G(2) are subject to sunset clauses and are scheduled to "cease to have effect" in June this year.

The Bill seeks to extend these sunset provisions by a further 18 months.

Sunset clauses are included in legislation for a number of purposes, including:

- to ensure that certain legislative provisions only remain in operation as long as is necessary to address a temporary emergency situation;
- to compel the periodic review of the operation of a controversial provision, and
- to provide a temporary measure to respond to a particular problem, while a more permanent solution is developed.

In this case, the sunset clauses fulfil the third purpose. The purpose of sections 5F(2) and 5G(2) is to provide an interim measure to ensure Commonwealth agencies' network protection systems are not in breach of the TIA Act, while a more permanent solution to the problem is developed.

The Law Council is not in a position to comment on either necessity for, nor potential perils of the exemption provided for by sections 5F(2) and 5G(2).

The Law Council notes only that parliament should be reluctant to extend the relevant sunset clauses without first inquiring about what progress has been made in designing a more permanent solution, why it is not in place already and whether and why a further eighteen months is required.

---

[3] The exemption provisions were originally limited to the AFP, however, the *Telecommunications (Interception and Access) Amendment Bill 2007* extended the exemption provisions to apply to the Australian Commission for Law Enforcement Integrity and the Australian Crime Commission), security authorities (ASIO, the Department of Defence, the Department of Foreign Affairs and Trade) and eligible authorities of a state (police forces and integrity commissions), all of which are defined in subsection 5(1).

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.