Law Council
OF AUSTRALIA

Telecommunications (Interception and Access) Bill 2007

Senate Legal and Constitutional Affairs Committee

July 2007

GPO Box 1989, Canberra, ACT 2601, DX 5719 Canberra
Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639
19 Torrens St Braddon ACT 2612
www.lawcouncil.asn.au

Table of Contents

Introduction

The *Telecommunications (Interception and Access) Bill 2007* furthers the consolidation in one Act, the *Telecommunications (Interception and Access* Act 1979 ("the TIA Act"), of legislative provisions regulating access to telecommunications information by enforcement agencies. To that extent, the Law Council believes it represents a positive development.

However, the Law Council has concerns about certain provisions of the Bill which lack clarity or which provide insufficient safeguards against the misuse or overuse of authorisation powers that allow for covert access to private information.

Although, a range of enforcement agencies already have access, without a warrant, to telecommunications data, the highly personal nature of such data should not be underestimated and access to it ought to be tightly controlled and monitored.

While telecommunications data does not include the content and substance of a person's private communications, it nonetheless reveals information about crucial matters such as their associations and their whereabouts.

On that basis the Law Council provides the following comments on the Bill.

Voluntary Disclosure

An improvement on the existing provisions

Under ss276, 277 and 278 of the *Telecommunications Act 1997,* there is a broad prohibition, enforced by criminal sanction, on carriers, carriage service providers, number data-base operators, emergency call persons and their respective associates disclosing information about:

- the contents of communications that have been, or are being, carried by carriers or carriage service providers;
- carriage services supplied; and
- the affairs or personal particulars of other persons.

The Bill seeks to introduce into the *TIA Act* new provisions which would allow, in certain circumstances, an employee of a carrier or carriage service provider to voluntarily disclose telecommunications data, without offending against ss276, 277 and 278 of the *Telecommunications Act*. Specifically, the Bill provides that:

- a person may voluntarily disclose telecommunications data to ASIO ***if the disclosure is in connection with the performance by ASIO of its functions (proposed s 174);*** and

- a person may voluntarily disclose telecommunications data to an enforcement agency ***if the disclosure is reasonably necessary for the enforcement of the criminal law (proposed* s177(1));** and

- a person may voluntarily disclose telecommunications data to an enforcement agency ***if the disclosure is reasonably necessary for the enforcement of a***

law imposing a pecuniary penalty or for the protection of the public revenue. (proposed s177(2)).

These proposed provisions are similar to existing exemption provisions in the *Telecommunications Act*, which will be repealed if the Bill is passed. The key difference is that under the amended *TIA Act,* as amended by the Bill, it will be explicitly stated that the voluntary disclosure exemption provisions do not cover:

- the disclosure of the substance or contents of a communication;[1] and
- the disclosure of telecommunications data which is informally requested by ASIO or an enforcement agency but the disclosure of which has not been formally authorised by that an agency.[2]

The Law Council believes that the new provisions that the Bill seeks to introduce into the *TIA Act* are a positive development and improve the integrity of the telecommunications interception and access regime.

The Law Council welcomes the clearer and tighter restrictions on voluntary disclosure of telecommunications information.

Voluntary Disclosure to ASIO

While acknowledging the proposed provisions are an improvement on the existing law, the Law Council also believes that s174 requires further refinement if it is to effectively guide employees of carrier or carriage service providers about when they may lawfully, voluntarily and in an unsolicited manner disclose telecommunications data to ASIO.

Under proposed section 174 of the *TIA Act*, as under the existing voluntary disclosure provisions of the *Telecommunications Act*, voluntary disclosure of telecommunications data to ASIO is permissible if it is "in connection with the performance by the organisation of its functions."

Those functions are listed in s17 of the *ASIO Act 1979* as follows:

(1) The functions of the Organisation are:

(a) to obtain, correlate and evaluate intelligence relevant to security;

(b) for purposes relevant to security and not otherwise, to communicate any such intelligence to such persons, and in such manner, as are appropriate to those purposes;

(c) to advise Ministers and authorities of the Commonwealth in respect of matters relating to security, in so far as those matters are relevant to their functions and responsibilities;

(ca) to furnish security assessments to a State or an authority of a State in accordance with paragraph 40(1)(b);

[1] S172

[2] S174(2) and s177(3)

(d) to advise Ministers, authorities of the Commonwealth and such other persons as the Minister, by notice in writing given to the Director-General, determines on matters relating to protective security; and

(e) to obtain within Australia foreign intelligence pursuant to section 27A or 27B of this Act or section 11A, 11B or 11C of the Telecommunications (Interception and Access) Act 1979 , and to communicate any such intelligence in accordance with this Act or the Telecommunications (Interception and Access) Act 1979 .

(2) It is not a function of the Organisation to carry out or enforce measures for security within an authority of the Commonwealth.

Given this long and complex list of functions, the Law Council believes that the threshold test applied by section 174 (that is, that the disclosure must be "in connection with the performance by ASIO of is functions) is a very difficult test for a person outside of ASIO to apply.

This may not have been a problem under the existing provision (s283(1) of the *Telecommunications Act*) because the voluntary disclosure of information may not have been limited to unsolicited disclosure.

Recommendation: In order to provide appropriate and clear guidance and parameters, the Law Council believes that s174 should be amended to state more explicitly the circumstances in which voluntary disclosure of telecommunication data to ASIO is not prohibited.

For example it may be necessary to specify that voluntary disclosure is permissible if "it will assist ASIO in obtaining intelligence that is relevant to

(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:

(i) espionage;

(ii) sabotage;

(iii) politically motivated violence;

(iv) promotion of communal violence;

(v) attacks on Australia's defence system; or

(vi) acts of foreign interference; whether directed from, or committed within, Australia or not; and

(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a).

Access to telecommunications data on a prospective basis

Unlike many other provisions of the Bill, proposed Sections 176 and 180, do not involve the transfer and refinement of existing provisions from the *Telecommunications Act.* On the contrary, they allow ASIO and criminal law enforcement agencies access to

telecommunications data on an entirely new basis. The Law Council believes that they are the most concerning provisions proposed by the Bill.

Section 176 allows an eligible person within ASIO to authorise the disclosure of prospective telecommunications data to ASIO, on a near real-time, ongoing basis for a period of 90 days. In order to issue such an authorisation, the eligible person within ASIO need only be satisfied that the disclosure would be in connection with the performance by ASIO of its functions.

Section 180 allows an authorised officer within a criminal law-enforcement agency to authorise the disclosure of prospective telecommunications data to that agency, on a near real-time, ongoing basis for a period of 45 days. In order to issue such an authorisation, the authorised officer must be satisfied that the disclosure is reasonably necessary for the investigation of an offence that is punishable by imprisonment for at least 3 years. The authorised officer must also "*have regard to*" how much the privacy of any person or persons would be likely to be interfered with by the disclosure.

In the case of mobile phones, telecommunications data includes information not only about who the user has communicated with, when and for how long; it also includes accurate information about the user's location. Thus, the effect of s176 and s180 is to grant ASIO and criminal law-enforcement agencies the ability to use a person's mobile phone, effectively, as a tracking device.

It is acknowledged in the Explanatory Memorandum (EM) that there are "increased privacy implications" in authorising the disclosure of telecommunications data on a near real-time, ongoing basis. For that reason, the Bill provides that:

- not all enforcement agencies are able to authorise disclosure of prospective information;

- only a more restricted class of person within ASIO may authorise such a disclosure; and

- in the case of criminal law-enforcement agencies, a more stringent threshold test is required than in the case of an ordinary authorisation.

Nonetheless, the Law Council believes that these restrictions do not offer adequate safeguards against abuse or overuse of the intrusive power effectively granted by ss176 and 180.

Authorisation for access to prospective telecommunications data for criminal law-enforcement agencies

Requirement to Obtain a Warrant

Given the invasion of privacy it represents, the Law Council believes that criminal law-enforcement agencies should require a warrant in order to access prospective telecommunications data and thus use a person's mobile phone as a tracking device.

The Law Council recognises that under Section 39 of the *Surveillance Devices Act 2004*, law enforcement officers are already able to use a tracking device without a warrant in the investigation of a federal offence which carries a maximum penalty of at

least 3 years.[3] This is provided that written permission is received from an "appropriate authorising officer" and installation and retrieval of the device does not require entry onto premises without permission or interference with the interior of a vehicle without permission.[4]

Nonetheless, the Law Council believes that the ease with which telecommunications data may be used to track a person, as compared to the difficult of secretly affixing a physical tracking device to a person or thing, renders proposed s 180 far more amenable to misuse or overuse by law enforcement agencies than existing provisions in the *Surveillance Devices Act 2004.*

It is on that basis that the Law Council believes that access to prospective telecommunications data should require a warrant.

Recommendation: A warrant should be required in order for a criminal law-enforcement agency to be granted access to prospective telecommunications data which may be used to track a person.

The Authorisation Process

In the event that the Bill is not amended to require a warrant, the Law Council believes that the authorisation process set out in proposed s180 should be amended so that they are at least as stringent, if not more stringent, than those found in section 39 of the *Surveillance Devices Act 2004.*

According to the Law Council, this would require:

(a) that only an "appropriate authorising officer" as defined in section 6 of the *Surveillance Devices Act* may authorise the disclosure of prospective telecommunications data. (In the case of most, if not all, agencies which will be listed in the *TIA Act* as criminal law-enforcement agencies this would appear to limit the class of persons who may authorise disclosure of prospective telecommunications data to a much narrower group.)

(b) that the officer requesting authorisation must apply in writing[5] to the "appropriate authorising officer" addressing the following matters:

   i. the name of the applicant; and

   ii. the duration of the authorisation sought; and

   iii. the reasonable grounds on which the authorisation is sought, being the grounds on which the officer suspects that:

      - one or more relevant offences have been, are being, are about to be, or are likely to be, committed; and

[3] And certain other federal offences listed in the definition of "relevant offence" in section 6 of the Surveillance Devices Act 2004.

[4] Sections 39(1) and 39(8) *Surveillance Devices Act 2004*

[5] Section 39 allows for oral applications but the Law Council believes that this does not allow for an appropriate level of transparency, accountability and oversight.

- an investigation into those offences is being, will be, or is likely to be, conducted; and

- access to prospective telecommunications data is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the commission of the relevant offences or the identity or location of the offenders.

The Law Council notes that the permission to use a tracking device granted under s39 of the *Surveillance Devices Act 2004* may extend for a period of up to 90 days. The Law Council does not recommend that the period of 45 days proposed in the current Bill be extended.

Recommendation: If a warrant is not required, the authorisation process in relation to the disclosure of prospective telecommunications data should be at least as stringent as that provided for under s 39 of the Surveillance Devices Act 2004.

Threshold Test in Relation to Privacy

Proposed section 180(5) currently requires that, before authorising disclosure of prospective telecommunication data, an authorised officer "must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure."

As currently drafted this subsection has little value. It is not clear what it means to "*have regard to*" a person's privacy. How is this intended to impact upon or guide the decision maker in this context?

The Law Council believes that the section should be amended so that it is expressed in terms of a test to be applied by the authorised officer. The Law Council suggests, for example, that the subsection could provide as follows:

"Before making the authorisation, the appropriate authorising officer must be satisfied on reasonable grounds that the likely benefit to the criminal investigation which will result from the disclosure *substantially* outweighs the extent to which the disclosure is likely to interfere with the privacy of any person or persons."

Recommendation: If a warrant is not required, section 180(5) should be amended to require authorising officers to address a more specific threshold test in relation to privacy.

Secondary Disclosure of Prospective Telecommunications Data

As noted above, the Bill proposes that enforcement agencies, like the ATO or ASIC, whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue, will be unable to issue a s180 disclosure authorisation. This is said to operate as a limit on the inappropriate use or overuse of the intrusive tracking power.

As also noted above, the Bill further proposes that a s180 disclosure authorisation will only be available in relation to the investigation of certain criminal offences. It will not,

for example, be available merely for the purpose of enforcing a law which imposes a pecuniary penalty or for the protection of the public revenue.

These limitations are thwarted, however, if information obtained pursuant to s180 can be shared, in near real-time, amongst all types of enforcement agencies for a wide variety of purposes.

As currently drafted s182(2) and (3) allow telecommunications data obtained pursuant to s180 to be shared and used on this largely unlimited basis and need to be amended accordingly.

Recommendation: The Secondary Disclosure provisions in s182 should not allow a criminal law-enforcement agency to disclose information obtained under a s180 authorisation to an agency which is not itself able to authorise and access prospective telecommunications data.

Likewise, the secondary disclosure provisions in s182 should not allow a criminal law-enforcement agency to disclose information obtained under a s180 authorisation for a purpose which is not itself capable of providing grounds for a s180 authorisation.

Reporting Requirements

The Law Council also believes that the reporting obligations associated with authorisations for access to prospective telecommunications data should be amended so that they are at least as stringent, if not more stringent, than those set out in s 50 of the *Surveillance Devices Act.*

According to the Law Council this would require amending proposed section 186 to provide that each criminal law-enforcement agency, in addition to reporting to the Minister each year how many authorisations were issued under s180, would also have to report:

(a) the number of applications for authorisation that were refused during that year, and the reasons for refusal; and

(b) the number of arrests made by officers of the agency during that year on the basis (wholly or partly) of telecommunication data obtained under a prospective authorisation issued under s180; and

(c) the number of prosecutions for relevant offences that were commenced during that year in which information obtained as a result of telecommunication data disclosed under a prospective authorisation issued under s180 was given in evidence and the number of those prosecutions in which a person was found guilty.

Consistent with s 52(f) of the *Surveillance Devices Act,* the Law Council also believes that criminal law-enforcement agencies should be required to keep a record of the details of each communication by an officer of that agency to a person other than an

officer of that agency of telecommunications data obtained pursuant to a prospective authorisation issued under s180.[6]

Recommendation: The reporting requirements for s180 authorisations should be at least as stringent as those required by s 50 of the Surveillance Devices Act 2004

Authorisation for access to prospective telecommunications data for ASIO

As with criminal law-enforcement agencies, the Law Council believes that ASIO should require a warrant in order to access prospective telecommunications data and thus use a person's mobile phone as a tracking device.

With respect to ASIO, the case against "warrantless" access to prospective telecommunications data is even stronger, given that at present ASIO can not use a tracking device without a warrant issued by the Minister.

Section s26A of the *ASIO Act* provides as follows:

> *Unlawful use of tracking devices*
>
> *(1) Subject to subsection (2), it is unlawful for an officer, employee or agent of the Organisation to use a tracking device for the purpose of tracking a person or an object. It is the duty of the Director-General to take all reasonable steps to ensure that this subsection is not contravened.*
>
> *Lawful use of tracking device*
>
> *(2) Despite any law of a State or Territory, an officer, employee or agent of the Organisation does not act unlawfully, by using, for the purposes of the Organisation, a tracking device for the purpose of tracking a person or an object if:*
>
> *(a) the person, or the person using the object, consents to it being done; or*
>
> (b) *the officer, employee or agent of the Organisation does so in accordance with a warrant issued under section 26B or 26C.*

Sections 26B and C provide that ASIO tracking device warrants may only be:

- issued by the Minister,
- issued in order to track a person engaged in or reasonably suspected by the Director-General of ASIO of being engaged in or of being likely to engage in, activities prejudicial to security; and
- issued if the device will, or is likely to, assist the ASIO in carrying out its function of obtaining intelligence relevant to security.

[6] The Law Council notes that under section 306A, to be inserted into the Telecommunications Act by the Bill, carriers, carriage service providers and number-database operators are already required to record disclosures made pursuant to a prospective authorisation.

The Law Council acknowledges that these warrants extend for up to six months and authorise a range of ancillary acts necessary for planting and maintaining the tracking device.

Nonetheless, the Law Council does not believe that the tracking of a person facilitated by proposed s176 of the *TIA Act* is so markedly different from and less invasive of a person's privacy than, what is permitted under s26B and C, that it should be allowed to occur without a warrant at all.

For that reason the Law Council believes that s176 should be amended to require that, in order to obtain access to prospective telecommunications data, ASIO must attain a warrant from the Minister, which the Minister must only issue if satisfied that:

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

- the disclosure of the prospective telecommunications data will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relevant to security.

Record keeping and reporting obligations, which are consistent with those provided for in ss32 and 34 of the *ASIO Act,* should attach to the issue of these warrants.

Records produced should be subject to review by the Inspector General of Intelligence in the same manner that records produced in connection with tracking device warrants are subject to review by the Inspector.

Recommendation: A warrant should be required in order for ASIO to be granted access to prospective telecommunications data which may be used to track a person.

Record keeping and reporting obligations, which are consistent with those provided for in ss32 and 34 of the ASIO Act, should attach to the issue of these warrants.

Records produced should be subject to review by the Inspector General of Intelligence in the same manner that records produced in connection with tracking device warrants are subject to review by the Inspector.

General Observations on the Authorisation Process

<u>Enforcement Agencies limited to authorising disclosures relevant to the performance of their functions</u>

Proposed Division 4 allows disclosure of telecommunications data for three purposes:

- when it is reasonably necessary for the enforcement of the criminal law;

- when it is reasonably necessary for the enforcement of a law imposing a pecuniary penalty; and

- when it is reasonably necessary for the protection of the public revenue.

Proposed section 178 and 179 allow all "enforcement agencies", regardless of their function, to authorise the disclosure of telecommunications data for all three purposes.

The Law Council does not believe that the Bill should allow agencies to authorise the disclosure of information for a purpose which is beyond their mandate. The Law Council questions how an agency could be satisfied that a disclosure was "reasonably necessary" for a purpose unrelated to the agency's functions.

Recommendation: Proposed section 178(3) and proposed section 179(3) should be amended to add "and is in connection with his or her agency's performance of its functions."

Form of Authorisations

The Law Council notes that the form that authorisations will take under proposed Division 3 and 4 will be largely determined by the Communications Access Coordinator, in consultation with the Privacy Commissioner and the Australian Communications and Media Authority.

Provisions regulating the form and content of authorisations will be key to maintaining the integrity of the regime and facilitating meaningful and reviewable record-keeping practices.

The Law Council would welcome the opportunity to consult with the Communications Access Coordinator on this matter.

Prohibitions on Secondary Disclosure and Use

The Law Council does not understand, nor does the EM explain, why the prohibition on secondary use or disclosure of telecommunications data contained in proposed s182(1) is not extended to ASIO.

It may be that there are provisions in the *ASIO Act* or other legislation which already broadly prohibit this type of secondary use or disclosure. If there is no alternative prohibition in place, the Law Council believes that proposed 182(1) should be amended accordingly.

Recommendation: The general prohibition in section 182(1) on secondary use or disclosure of telecommunications data which has been disclosed to a person pursuant to Division 4, should also apply to telecommunications data disclosed to ASIO pursuant to Division 3.

Definitions – Amendments to Section 5(1) of the *TIA Act*.

Definition of Criminal Law Enforcement Agency

Clause 4 inserts into section 5(1) of the *TIA Act* a definition of "criminal law enforcement agency".

This definition is significant because amongst the broader group of "enforcement agencies" able to access telecommunications data under the *TIA Act*, only "criminal law enforcement agencies" are granted access to telecommunications data on a prospective basis.

Clause 4 defines "criminal law enforcement agency" as "a body covered by any of the paragraphs (a) to (k) of the definition of 'enforcement agency'".

Thus, in effect, "criminal law enforcement agency" is defined as:

(a) the Australian Federal Police; or

(b) a police force or service of a State; or

(c) the Australian Commission for Law Enforcement Integrity; or

(d) the ACC; or

(e) the Crime Commission; or

(f) the Independent Commission Against Corruption; or

(g) the Police Integrity Commission; or

(h) the Office of Police Integrity; or

(i) the Crime and Misconduct Commission; or

(j) the Corruption and Crime Commission; or

(k) **an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purposes of this paragraph.** .(emphasis added)

The Law Council believes there is no need for paragraph (k) to be included in the definition. The definition is intended to operate as a safeguard, providing a clear limit on the agencies which have access to an extraordinary and invasive power.

The Law Council believes that the practice of reserving to the Executive the power to expand definitions of this nature, which are crucial to scope and operation of the *TIA Act*, is of great concern. No reason has been provided for why the efficient operation of the *TIA Act* requires the sort of flexibility afforded the Executive under paragraph (k).

Recommendation: The definition of "criminal law enforcement agency" proposed in clause 4 should be amended by deleting paragraph (k) from the definition of "enforcement agency" proposed in clause 6.

Definition of Enforcement Agency

Clause 6 repeals the existing definition of "enforcement agency" and replaces it with a new definition

In effect the new definition is essentially the same as the existing definition except that previously it included:

"a body or organisation responsible to the Australasian Police Ministers' Council for the facilitation of national law enforcement support; and includes the National Exchange of Police Information".

Reflecting organisational or administrative changes, the definition now includes instead at paragraphs (l) and (m):

"(l) a body or organisation responsible to the Ministerial Council for Police and Emergency Management - Police; and

(m) The CrimTrac Agency".

Together with the name change, it is, importantly, now also acknowledged by the Bill that the agencies or bodies referred to in paragraphs (l) and (m) are not criminal law-enforcement agencies, as they were previously described in section 282 of the Telecommunications Act and as they were described in an exposure draft of the current Bill.

Similarly, it is clear from the Bill that the agencies or bodies referred to in paragraphs (l) and (m) do not fall into the two other categories of "enforcement agency", that is, bodies whose functions include administering a law imposing a pecuniary penalty and bodies whose functions include administering a law relating to the protection of the public revenue.

On that basis, the Law Council questions whether paragraphs (l) and (m) should remain in the definition of an enforcement agency. Enforcement agencies have significant and intrusive powers. They are able to apply for stored communication warrants and authorise the disclosure of telecommunications data.

Unless a compelling case can be made for why the agencies or bodies referred to in paragraphs (l) and (m) should remain within the definition of an enforcement agency, notwithstanding that they are not criminal-law enforcement agencies and do not administer a law imposing a pecuniary penalty or a law relating to the protection of the public revenue, they should be removed. Agencies should never be included within key legislative definitions on the basis of which powers are conferred merely as a default or "catch all" mechanism.

Recommendation: Unless a compelling case can be made for why the agencies or bodies referred to in paragraphs (l) and (m) should remain within the definition of an enforcement agency, notwithstanding that they are not criminal law-enforcement agencies and do not administer a law imposing a pecuniary penalty or a law relating to the protection of the public revenue, they should be removed.

Absence of Key Definition

The new Chapter 4 that the Bill seeks to insert into the *TIA Act* is headed "Access to Telecommunications Data". However, the term "telecommunications data" is not defined in the Bill and is not defined in the existing *TIA Act* or the *Telecommunications Act.*.

The key provisions of the Chapter, from a law enforcement perspective, are concerned with the disclosure and use of information and documents which are not and do not contain the contents or substance of a communication. Such information and

documents are assumed to be what is meant “telecommunications data” although this is not spelt out in the Bill.

The EM is a little more precise. It provides that:

> *“Telecommunications data is information about a telecommunication, but does not include the content or substance of the communication. Telecommunications data is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet based applications including internet browsing and voice over internet telephony.*
>
> *For telephone-based communications, telecommunications data includes subscriber information, the telephone numbers of the parties involved, the time of the call and its duration. In relation to internet based applications, telecommunications data includes the Internet Protocol (IP) address used for the session, the websites visited, and the start and finish time of each session.*
>
> *Telecommunications data specifically excludes the content or substance of a communication.”*

Thus the working definition of telecommunications data derived from the EM defines the term by what it is not: it is information about a telecommunication that does not include the content or substance of the communication.

This definition is workable only insofar as there is a clear distinction between the contents or substance of a communication and all other information about the communication.

The Law Council believes that such a distinction can not necessarily be drawn. For example, submissions on the Exposure Draft of the Bill revealed that there remains room for debate about whether the address of a webpage, which may reveal a great deal about the contents of the page, falls into the “substance and contents” category or the residual “telecommunication data” category.

The purpose of the Bill is to consolidate and refine the legislative provisions which set out the circumstances in which different types of telecommunications information can be disclosed and accessed for law enforcement purposes.

It is assumed that one of the key aims of the exercise is to ensure that both the privacy rights of individuals and the powers of enforcement agencies are clearly understood. It seems unfortunate, and possibly counterproductive, in those circumstances not to properly define “telecommunications data”.

Recommendation: Given that the provisions introduced into the TIA Act by the Bill allow a diverse range of agencies for a diverse range of purposes to covertly access telecommunications data without warrant, the Law Council believes that the Bill should set out in positive terms exactly what type of personal information is encompassed within the meaning of that phrase.

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.

GPO Box 1989, Canberra, ACT 2601, DX 5719 Canberra | Telephone **+61 2 6246 3788** Facsimile +61 2 6248 0639 | 19 Torrens St Braddon ACT 2612 www.lawcouncil.asn.au