Australian Government
Attorney-General's Department

Security and Critical
Infrastructure Division

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

Email: legcon.sen@aph.gov.au

Dear Secretary

**Inquiry into the provisions of the Telecommunications (Interception and Access) Amendment Bill 2007 – answers to questions on notice**

During the Committee's public hearing on Monday 16 July 2007, the Department took a number of questions on notice. The Committee Secretariat subsequently sent a number of additional questions.

Following are the Department's responses to these questions.

The contact officer in the Branch is Jonathan Curtis who may be contacted on 6250 6359.

Yours sincerely

Catherine Smith
Assistant Secretary
Telecommunications and Surveillance Law Branch

July 2007

# Inquiry into the provisions of the Telecommunications (Interception and Access) Amendment Bill 2007

## Answers to questions on notice

Please note that in this document, the Telecommunications (Interception and Access) Act 1979 is referred to as the TIA Act. The Telecommunications (Interception and Access) Amendment Bill 2007 is referred to as the Bill. The Telecommunications Act 1997 is referred to as the Telecommunications Act.

***Process***

1. The Attorney-General has foreshadowed some more amendments to the TIA Act as a result of the committee's recommendations to the 2006 Bill. When are these likely to be tabled?

And

*3. The Committee has received the Government's response to the 2006 amendments. When will the Government implement any remaining amendments as a result of accepting some of the 2006 report recommendations?*

The Government tabled its response to the Committee's report on 10 May 2007. Only three matters contained in the government response are yet to be finalised. The relevant parts are extracted below.

| |
|---|
| Recommendation 5 – The Committee recommends that the Bill be amended to allow issuing authorities to only include those currently able to issue interception warrants. |
| **Government response to Recommendation 5: Accepted for further consideration** |
| With the implementation of the stored communications warrant regime, it is necessary to expand the number of issuing authorities available for enforcement agencies to obtain a warrant where this is necessary. The ability for State Magistrates to be appointed as an issuing authority provides these additional resources, and parallels arrangements for general search warrant applications. |
| The Government accepts that there should be further consideration of this recommendation following a reasonable operational timeframe of the stored communications regime. |

Comment: This response remains current. The Government considers that a period of at least two years of operational experience is needed before there can be any meaningful review of the effectiveness of the stored communications regime. As the provisions came into force on 3 May 2006, the Department would expect to conduct such a review in the second half of 2008.

Recommendation 17 – The Committee recommends that prior to the passage of the Bill the definition of stored communications be amended so that the Australian Communications and Media Authority's ability to enforce the Spam Act is not limited.

**Government response to Recommendation 17: Accepted**

The provisions allowing Australian Communications and Media Authority officers' access to stored communications as part of their function of enforcing the *Spam Act 2003* were substantially implemented in the Bill. The Government accepts that the stored communications regime should not adversely impact upon the enforcement of the *Spam* Act, and will ensure that the regime does not impede those enforcement objectives.

Comment: The Department notes that, in addition to the amendments to the Telecommunications (Interception) Amendment Act 2006 outlined above, the current Bill contains an additional provision at Item 20 of Schedule 2 that amends section 139 of the TIA Act to permit secondary disclosure of stored communications for the purposes of a proceeding under the Spam Act 2003.

Recommendation 26 – The Committee recommends 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.

**Government response to Recommendation 26: Accepted**

The Government supports the use of unique identifiers as the basis for access to communications. 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.

Comment: There are two equipment identifiers that are currently used for these purposes:

- IMEI International Mobile Equipment Identity (a unique number identifying every GSM and UMTS mobile phone)
- MAC Media Access Control (a number identifying every piece of hardware)

Government agencies continue to develop systems to utilise these and other numbering systems. As these identifiers are developed by international bodies, and

are evolving continually, the Government considers that it would be prudent to move any necessary amendments at a later date.

*2. Should we be amending the TIA Act before a review of the 2006 amendments has taken place?*

Yes. The 2006 amendments, which created the stored communications warrant regime and made provision for B-Party telecommunications interception warrants, represented the implementation of the first tranche of recommendations arising from the Blunn Report into the Review of access to telecommunications. The current bill, in moving provisions from the Telecommunications Act to the TIA Act, implements the bulk of the remaining recommendations. As such the bills contain separate and independent provisions and consideration of the second bill is in no way dependent on an evaluation of the first.

*4. The amendments in this Bill were the subject of a consultation process by way of comment on an exposure draft. Can you explain how the Bill addresses the feedback that was received during this consultation process? Outline in particular how the issues raised by AMTA, Telstra and the Privacy Commissioner were addressed.*

<u>AMTA, Telstra and the telecommunications industry</u>

The issue of greatest concern to industry was the proposed Attorney-General's Determination making powers contained in @192 of the Exposure Draft of the Bill. These concerns were founded on the fact that obligations relating to interception capability created pursuant to this power must be complied with at the carrier's expense. Carriers argued that there was insufficient justification of the need for this power. Carriers were also concerned that Determinations could have been used to create unique Australian-specific standards entailing high compliance costs; and that the consultation provisions in the proposal were inadequate.

Based on these concerns, Government decided to remove the proposed determination making power for interception capability and instead transfer the existing Determination making power in Section 322 of the Telecommunications Act into the TIA Act.

<u>Telstra also suggested:</u>

More extensive consultation prior to the release of CAC determinations in relation to delivery capability: The Government partially agreed. Before making a declaration, the Communications Access Co-ordinator (the CAC) must consult with ACMA, which provides an opportunity for industry views to be raised. However, formal consultation provisions have been limited because the costs of any measures contained in the determination are to be paid for by the agencies.

*Confirmation that authorisations are conclusive on their face*: the Government agreed with the intent of this recommendation. However legislative amendments were considered unnecessary since disclosures made by a carrier are covered by the good faith provisions in subsection 313(5) of the Telecommunications Act.

Privacy Commissioner

The Office of the Privacy Commissioner generally supported the provisions of the Exposure Draft, but made several recommendations, including:

*Clarifying voluntary disclosure provisions:* Defining the term 'call data', or giving examples in the EM. For the reasons set out in the public hearing, the Government considers it would be impractical to attempt to define 'telecommunications data' in the legislation. However, the suggestion to provide examples in the EM was agreed to and is reflected in the final document.

*Giving guidance on how the privacy of telecommunications users should be taken into account.* The Government did not agree with the recommendation to include further legislative guidance on consideration of privacy. Consideration of privacy issues will vary enormously according to the unique circumstances of each situation. In particular, this may include the relationship between the seriousness of the offences being investigated, the value of information likely to be obtained, and the extent to which accessing this information would, in the circumstances, breach an individual's privacy.

However, these are matters that the CAC may wish to address in the procedural requirements provided for in new section 183.

*The operation of the TIA Act should be subject to review every five years:*
The Government does not agree to a requirement mandating formal review in this way. As the experience of the past ten years demonstrates, the legislation is subject to near constant operational review, leading to regular legislative amendments and associated Parliamentary and public scrutiny, including through Parliamentary Committee inquiries. This has included formal reviews of the regime governing interception and industry obligations to assist that were undertaken by Mr Pat Barrett, Mr Dale Boucher, Mr Peter Ford, Mr Tom Sherman and Mr Anthony Blunn, as well as five Senate Committee legislative inquiries. As such, any mandatory statutory review process is unnecessary.

*5. Telstra's concerns*

*The lack of industry consultation required prior to any Ministerial or CAC Determination:*

Industry consultation was part of the *Report of the Review of the Regulation of Access to Communications* by AS Blunn AO but during the consultation phase of the exposure draft a consensus could not be reached on determinations. It was therefore agreed to transfer the existing determination making power under section 322 of the Telecommunications Act and to include 'Matters to be taken into account' in the Bill.

The Government believes that industry consultation is unnecessary for CAC determinations on delivery capabilities because the cost for agency specific delivery capability is a cost to be borne by the intercepting agencies. All consultation on agency specific delivery requirements is performed in contract negotiation between the lead agency and the carrier.

*The use of new terminology for interception capability which causes confusion as to the scope of responsibility of carriers in relation to providing such capability:*

This provision is a direct transfer of the existing definition of interception capability used in the Telecommunications Act. The slight differences in language are intended to ensure consistency with the terminology already used in the TIA Act.

The obligation for interception capability relates to the ability to intercept the *communication* travelling over the network, facility or carriage service (telecommunications service). The obligation does not relate to whether the communication is a carriage service, a content service or what particular equipment it should relate to.

If anything, the definition limits interception capability by excluding radio communications equipment.

*Expanding the matters to be taken into account by the Minister and the CAC prior to making a determination and by the CAC in deciding whether to grant an exemption:*

Ms Smith from the Attorney-General's Department makes reference to *Matters to be taken into account* by the Minister and CAC making determinations as part of her evidence in the Proof Committee Hansard on page 28.

*Requiring the CAC and ACMA to give reasons for the rejection of any exemption request and establishing an appeals process:*

Ms Smith from the Attorney-General's Department makes reference to the Exemption process as part of her evidence in the Proof Committee Hansard on page 29.

Consistent with the current legislation, the Bill provides a mechanism for carriers and carriage service providers to apply to the CAC for an exemption from some or all interception capability obligations under the Act.

There are various reasons why the CAC may grant a carrier or carriage service provider with an exemption from some or all of its interception capability obligations. Essentially the CAC will consider the reasons for the request balanced against the obligations to provide interception capability.

The ACMA is also able to grant an exemption (s193) in relation to trial services were it is unlikely to create a risk to national security or law enforcement.

Where an exemption is granted, by either the CAC or ACMA, the exemption may be (and usually is) conditional and time restricted.

The 60 day time frame provides some certainty to industry that a request for an exemption should be finalised within that period.

There have not been any instances where a request for an exemption has not been responded to within the 60 day period with the average turn around timeframe being 30 days, which includes consultation with interception agencies.

Guidelines for Interception Capability Exemptions have been made available to Carriers and Carriage Service Providers for the specific reason of explaining what the Agency Co-ordinator (the current decision maker) takes into account when considering an exemption request.

*Removing the impractical effect of deemed exemptions caused by s.192(6):*

Ms Smith from the Attorney-General's Department makes reference to the 'validity period of exemption' as part of her evidence in the Proof Committee Hansard on pages 29 and 30.

*Clarifying the definition of "Interception Capability" and obligation on carriers in s.191 to ensure the scope of interception obligations on carriers remain identical to that currently under the Telco Act.*

Ms Smith and Mr Markey from the Attorney-General's Department make reference to the definition of 'Interception Capability' as part of their evidence in the Proof Committee Hansard on page 29.

*Including delivery capability as a factor to be considered in determining Delivery Points:*

Mr Markey and Ms Smith from the Attorney-General's Department make reference to Delivery Points as part of their evidence in the Proof Committee Hansard on pages 27 and 28.

*Providing greater recognition of the privacy of our customers in respect of the issue of any authorisation:*

Measures in the Bill provide a balance between the requirements of national security and law enforcement and the privacy of the users of Australia's telecommunications systems, including the:

- continuation of an authorisation regime for the disclosure of telecommunications data
- clarification of the voluntary disclosure provisions
- clarification of the prohibitions on the disclosure of the contents and substance of a communication under new Chapter 4
- distinction made between access to historical and prospective information
- requirement for authorised officers to have regard to privacy considerations when making prospective authorisations
- requirement to revoke a prospective authorisation where the disclosure is no longer required
- inclusion of record keeping and reporting requirements for agencies, and
- inclusion of offences for the secondary disclosure and/or use of telecommunications information, except in defined circumstances.

*Clarifying the pecuniary penalty and protection of public revenue bodies caught under the definition of "enforcement agency":*

Under current laws, both Commonwealth and State and Territory agencies that administer a law imposing a pecuniary penalty or protecting the public revenue may access telecommunications data. The Bill maintains this position. Given the wide range of agencies that are covered, it is impractical to list which agencies are included.

The additional requirement for the head of an agency to provide a copy of an authorisation, authorising relevant management positions, to the CAC will indicate

which agencies are covertly accessing telecommunications data. Any anomalies will be investigated by the CAC.

In practice, the Department will also provide a copy of these authorisations to carriers and carriage service providers that routinely receive requests for telecommunications data and any other industry participants that request them that will provide guidance as to which agencies will be requesting information.

*Clarifying in s.195(4) that any matters specified by the Minister to be included in a carrier's interception capability plan must only relate to reporting on matters relevant to a carrier's interception obligations.*

An interception capability plan is a written instrument that sets out how a carrier or nominated carriage service provider will comply with its interception capability obligations and address other relevant issues including business developments, and listing those employees who have responsibility for interception related matters. Any determination made by the Minister would necessarily be restricted to interception capability obligations as defined by the TIA Act or in accordance with any interception capability determinations made under proposed section 189 of the Bill.

*6. AMTA argues that any determination by the Australian Communications and Media Authority under section 188(5) or section 198(6) should be subject to appeal by the AAT. What is your response to this suggestion?*

All decisions made by the ACMA under the TIA Act are subject to judicial review pursuant to the *Administrative Decisions (Judicial Review) Act 1977*. For the Tribunal to assess the merits of a decision in relation to interception obligations or capability would require the public examination of the operational importance of particular types of communications and/or particular categories of information associated with those communications. This would necessitate the provision of public evidence pertaining to the telecommunications interception operation of agencies, and the limits of interception capability.

Where a decision is made under new subsection 188(5) and the circumstances of the carrier have changed materially, the carrier may nominate another delivery point under new subsection 188(8).

*7. AMTA argues that there should be a time limit of 180 days on the refusal of an exemption by the CAC under proposed subsection 192(6) or it should be repealed. What is the Department's view of these proposals?*

Ms Smith from the Attorney-General's Department makes reference to the Exemption process as part of her evidence in the Proof Committee Hansard on page 29.

*9. Does the AGD accept AMTA's comment that the list of requirements for the Interception Capability Plans are 'significantly' expanded?*

No. These provisions are consistent with the current provisions in the Telecommunications Act. The guidance provided in the EM lists a number of factors that are likely, if implemented, to effect interception capability. The particular reference in the EM to changes in marketing or pricing of services is referring to

instances where a carrier may offer free services or undertake major marketing campaigns with an expectation of substantially increasing their customer base, which is likely to have an impact on the ability to provide interception capability.

This can relate to both technical issues and or the corresponding increase in customer numbers and therefore the possibility of a larger number of interception warrants being implemented. For example, where a carrier packages products or services offered by other companies with their own products, the Communications Access Coordinator should be informed so discussions can be undertaken with the third party to ensure that the end to end service has interception capability.

***Definitions***

*10. Can you explain why there is need to allow delegated legislation to expand the definition of 'enforcement agency'? What possible agencies are intended to be included in the definition of 'enforcement agency' by regulation?*

The regulation making provision is a direct transfer from the Telecommunications Act which provides for an agency to be prescribed as a 'criminal-law enforcement agency'. While there are no agencies currently proposed to be prescribed, the regulation making power will allow the inclusion of agencies where their investigative functions change to the extent that access to prospective information becomes necessary.

For example, the Australian Customs Service and the Australian Securities and Investment Commission currently have access to historical data. If the nature of their investigative functions change to the extent that it is considered appropriate for them to receive telecommunications data in near-real time, they may be prescribed under paragraph 5(1)(k) of the TIA Act.

A regulation under paragraph 5(1)(k) is a disallowable instrument.

*11. The EM at page 8 suggests that the subject line of an email or details of internet sessions are not captured as 'telecommunications data' but is this clear under the provisions in the bill?*

While the term 'telecommunications data' is not defined in the Bill, it is effectively defined by exclusion, where section 172 states that Divisions 3 and 4 of Part 1 of the Bill do not authorise the disclosure of the contents or substance of a communication. Therefore, 'telecommunications data' can be regarded as information about a telecommunication, but does not include the content or substance of that communication.

Subject line of emails can include the substance or content of communication and therefore fall outside the definition of 'telecommunications data'.

*12. Do you agree with the OPC and EFA that there might sometimes be a blurring between content and data? If not, why not?*

Officers of the Department gave evidence on this matter in the Proof Committee Hansard at page 31.

The Department disagrees that the proposed provisions blur the line between content and data. The EM at page 8 states that 'the information does not include content such as the subject line of an email, the message sent by email or instant message or the details of Internet sessions'.

EFA in their submission provided an example that relates to user-defined 'headers' to email messages. EFA states that whilst headers generally do not contain personal information or content, there is the capacity to include information in headers which are defined by the user. They argue that there is therefore confusion as to whether this information is considered data or content.

The EFA rely on an Internet Engineering Task Force (IETF) standard referred to as Request for Comment (RFC) 822. This is an obsolete standard that was superseded in

2001 by RFC 2822 and the relevant header fields stated by EFA cannot be found in the current standard. RFC 2822 also states that these obsolete fields 'MUST NOT be generated'.

*13. The IGIS and EFA have questioned the inclusion of the 'conduct of the Commonwealth's international affairs' in the new definition of security authority. Could you explain why this phrase has been included in the definition?*

The definition of security authority in the Bill has a dual purpose in that it also defines which agencies are provided an exemption to the normal definition of 'passing over a telecommunications system' for the purposes of enforcing professional standards and protecting and maintaining highly secure networks. Agencies that have responsibilities for the conduct of the Commonwealth's international affairs are appropriately included within this definition. To obtain an authorisation for developing and testing interception capabilities, a security authority will still be required to demonstrate that it has functions that include activities relating to developing or testing technologies or interception capabilities.

*14. The Police Federation argue that the Bill erodes the privacy rights of police officers, especially in relation to the secondary disclosure provisions. They would like to see a narrow definition of 'pecuniary penalty' in the Bill or the reference deleted. In the alternative, they would like to see secondary disclosure provisions exempt disciplinary proceedings. What is your view of this suggestion?*

Mr Curtis gave evidence on this matter in the Proof Committee Hansard at page 22.

AGD has held detailed discussions with the Police Federation of Australia on this matter. The Department retains its view that the secondary disclosure provisions relating to telecommunications data are appropriate.

The Bill provides that it is an offence to disclose or use information lawfully obtained from a carrier unless the disclosure is reasonably necessary for:

- the performance by ASIO of its functions, or
- for the enforcement of the criminal law, a law imposing a pecuniary penalty and for the protection of the public revenue.

In practical terms the new provisions will allow agencies to share information internally where the information is of obvious relevance to another investigation being undertaken as long as the investigation in question is in relation to a criminal offence, a civil penalty offence or for the protection of the public revenue.

The PFA's principle objection to the provisions is that, because police are almost unique in having pecuniary penalties contained within their employment legislation, the secondary disclosure provisions of the Bill indirectly have greater impact on police than the general public.

However, the Department's view is that:

- Such secondary disclosure could only occur in circumstances in which the information could have been obtained under the primary disclosure rules.
- There is no specific provision enabling either the primary or secondary disclosure of telecommunications data relating to the investigation of police

misconduct. As such, the Bill would not create any provisions that are not of general application to the wider community, including police officers.

- Under the current legislation governing the employment of police in Australia, there is in fact little if any capacity to use this information in any police disciplinary investigations. This is by reason of the meaning of 'pecuniary penalty', which is limited to specific monetary penalties set out in relevant legislation and imposed by a court. The term does not include administrative sanctions that may have financial impact, such as for example, a demotion.
- The information in question is material already held by investigators, and which investigators pass on because it is known to contain evidence relevant to another investigation. It would be contrary to public policy to prevent its disclosure and use.

It should also be noted that secondary disclosed information would necessarily be available for the recipient enforcement agency to access in its own right, the differences being that the recipient agency may not be aware that the information exists, and if it does become aware of the information, it may no longer exist on the carrier's network. Additionally, the requirement for a further request for the same information would be duplication of effort to require the carrier to provide the same information twice.

To the extent that these provisions do indirectly have greater application to police than the public generally, it is may be justified by the greater accountability required of police. If the Police Federation considers that pecuniary penalties are inappropriately attached to minor misdemeanours, it is a matter that should pursued with their State/Territory Government.

For these reasons, the Department does not agree to the PFA's proposals.

In relation to their specific proposals:

*The proposal to delete or narrow the reference to 'pecuniary penalty'*: it must be remembered that these provisions apply to the operations of all types of government agencies and investigations at all levels of government. To amend the Bill as proposed, for the narrow purpose of limiting its effect on police disciplinary procedures, would therefore have much wider and unacceptable implications for the wider operation of the legislative regime.

*The proposal to amend the secondary disclosure provisions to exempt police disciplinary proceedings*: To accept this proposal would be contrary to public policy, since police disciplinary offences include matters that are of a serious nature for which relevant information should be disclosed. The only alternative would be to create special provisions limiting the type of police disciplinary proceedings for which disclosures would be permitted. This would unnecessarily increase the complexity of the legislative provisions and as noted above, the Government considers that it is a matter better dealt with under the relevant state and territory legislation.

*15. AMTA has suggested an amendment to Schedule 1, item 11, new section 6R regarding the requirement for the CAC to act in accordance with the objects of the Act. What is your view of this suggestion?*

Ms Smith from the Attorney-General's Department makes reference to the objects and regulatory policy of the Telecommunications Act by the Minister and CAC when making determinations as part of her evidence in the Proof Committee Hansard transcript at page 28.

*16. AMTA objects to the new definition of 'interception capability' in the Bill. Do you have any comment?*

Ms Smith and Mr Markey from the Attorney-General's Department discuss the definition of Interception Capability in their evidence in the Proof Committee Hansard at page 29.

*17. AMTA suggests that there should be a definition of 'intercept related information' inserted into section 5(1). What is your response to this proposal?*

Intercept related information is the same as 'telecommunications data' and therefore does not require a definition in section 5(1) of the Bill.

Intercept related information is a term used in European Telecommunications Standards Institute (ETSI) standards. A definition of 'intercept related information can be found in the standard – 'ETSI TS 101 331 V1.2.1 (2006-06), Lawful Interception (LI); Requirements of Law Enforcement Agencies'.

*18. EFA states in relation to historical data that:*

> Surveillance of web browsing activities is akin to filming individuals' activities in a manner that records every item they purchase in shops, every film they see at the cinema or hire or buy, every book and magazine they glance through and/or purchase or take out on loan from a library and so on. Furthermore, unlike "telecommunications data" about telephone calls and email messages, the address of a web page often, of itself, provides information about the content or substance of the communication and web page addresses can be used to obtain access to the content that was communicated.

*What is your response to this?*

The Department agrees with Electronic Frontiers Australia that the EM is ambiguous on page 6, Part 4-1 – 'Permitted access to telecommunications data' and page 8, Section 172 – 'No disclosure of the content or substance of the communication' with respect to names of websites being regarded as either content/substance of a communication or telecommunications data.

The Department has reviewed the EM and will propose that it be amended to remove the reference to the names of websites in the list of items included as telecommunications data.

However, the Department does not agree that telecommunications data relating to Internet sessions – such as IP addresses – provides content or a clear indication of the activities of a user. It is the view of the Department that the IP address of a website is

telecommunications data, as is an individual phone number. Whilst this may indicate the end user of either service, it does not indicate the activity of the individual at that site. It shows the origin and destination addresses of particular devices, but does not reveal in anything but the most general terms, the nature of the communication.

Access to an IP address is analogous to the knowledge gained from telephone number. For example, a telephone call to the switchboard of a large organisation shows the caller's interest in that organisation, but will not reveal which extension within the PABX system the caller was connected to.

Similarly, an IP address only indicates that an individual visited a specific internet page. It does indicate the activities occurring when that site was visited and it does not provide any details such as bank account numbers or internet passwords.

*19. EFA is also concerned by existing section 280, as described under paragraph 4.2, p. 12 of their submission no. 8. In their evidence to the Committee on 16 July Ms Graham stated that section 280 'muddies the waters' because it suggests that enforcement agencies can get access to stored communications by an ordinary search warrant. What is the Department's response? Does the section require amendment as the EFA suggest, and as this Committee has previously suggested?*

It is the Department's view that stored communications are only able to be covertly accessed via a carrier in accordance with the TIA Act. In accordance with the Legal Services Directions, the Department is unable to comment on the operation of legislation administered by another portfolio, but have forwarded your question to the Department of Communications, Information Technology and the Arts (DCITA).

DCITA have advised the Department that they consider that section 280 of the Telecommunications Act does not require amendment as Electronic Frontiers Association (EFA) have suggested, or as the Committee previously recommended. In DCITA's view, the submission provided by EFA does not reflect the distinct concepts: 'stored communications' under the TIA Act, and 'information or documents' and 'contents and substance of a communication' under Part 13 of the Telecommunications Act. DCITA considers that section 280 of the Telecommunications Act only provides an exception to the prohibition at sections 276, 277 and 278 of the Telecommunications Act. Those provisions provide for primary disclosure/use offences for eligible persons, eligible number-database operators and emergency call persons, respectively. These sections prohibit disclosure and use of information and documents and do not relate to stored communications, which are addressed in Chapter 3 of the TIA Act.

***Oversight***

*20. EFA thinks ASIO is getting a new power to access data, even though the second reading speech states otherwise. Could you respond to this concern?*

The Bill does not create new powers to access data. Existing laws permit carriers to disclose telecommunications data that is in existence and data that is generated in near-real time. Transferring these provisions from the Telecommunications Act to the TIA Act clarifies this situation and regulates the legality of access to such data.

ASIO currently access telecommunications data in accordance with section 283 of the Telecommunications Act, which enables disclosure of telecommunications data where the disclosure is made in connection with ASIO's functions.

*21. The IGIS has noted there may be a role for his office in monitoring approvals to access prospective data for ASIO. Do you agree? If not, why not?*

The Department agrees with the views given by the IGIS.

The *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) establishes the IGIS as an independent statutory officer with extensive powers to scrutinise actions of the intelligence and security agencies. The purpose of the oversight and review activities undertaken by the IGIS is to ensure that, among other things, each member of the Australian Intelligence Community, including ASIO, acts legally and with propriety, and complies with ministerial guidelines and directives.

The IGIS has access to all of ASIO's records and staff and may enter the agency premises at any time. Importantly, the IGIS has the power to inquire into public complaints, conduct inquiries referred by Government, and initiate inquiries. The IGIS regularly undertakes compliance inspections of ASIO's records and reports on his findings in the IGIS Annual Report.

Accordingly, the Department considers that the IGIS already has the necessary jurisdiction to oversight ASIO's use of the prospective data regime.

*22. Given that there is an expansion of powers under the Bill, would it be appropriate for ACLEI to have oversight of the exercise of the powers?*

As noted above, the Department does not agree that there is an expansion of powers under the Bill. This notwithstanding, the Department does not consider such a role for ACLEI to be appropriate. First, the accountability of the operation of the provisions is provided by means of the reporting regime and the administrative oversight provided by the Commonwealth and State Ombudsman's offices.

Second, ACLEI is an integrity agency with jurisdiction over agencies (the AFP and the ACC) rather than particular legislative provisions. To the extent that ACLEI were investigating one of these agencies, this scrutiny would extend to that agency's use of the powers to access telecommunications data.

*23. Privacy NSW has commented on the requirement in subsection 180(5) for an authorised officer to have regard to likely interference with the privacy of individuals when giving authorisation for access to prospective information or documents, and that paragraph 189(4)(c) provides, similarly, that the Minister, before making determinations in relation to interception capabilities, must take into account the privacy of the users of telecommunications systems. Privacy NSW has suggested proscribing (by way of regulation or similar) a requirement to have each enforcement agency (to whom authorising officers belong) develop guidelines on how the privacy implications of an authorisation should be considered and documented. What is your view of this proposal?*

See answer to Question 4 (Privacy Commissioner) above.

***Voluntary disclosure***

*24. The OPC has recommended that there should be a provision inserted into the Bill to mandate the destruction of any call data voluntarily disclosed to ASIO or law enforcement agencies (equivalent to existing section 79 of the TIA Act). What is your response to this recommendation?*

The Government will consider this recommendation, but notes reservations about the need for such an amendment.

*25. The Law Council feel that permitting voluntary disclosures to ASIO, 'if the disclosure is in connection with the performance by [ASIO] of its functions', is not enough guidance for people outside ASIO given the wide terms of section 17 of the ASIO Act. The Council suggests amending section 174 to spell out what sort of information might be relevant to ASIO, such as the protection of Australians from espionage, sabotage, politically motivated violence, etc. What is your response?*

The functions of ASIO are already set out in the ASIO Act (Part III – Functions and powers of the Organisation). The replication of these functions in the TIA Act is not considered necessary. In the Department's view, this definition in combination with the general understanding of ASIO's role is sufficient to enable a carrier or carriage service provider to form an accurate judgement as to the likely relevance of information to those functions.

*26. The Law Council thinks that the authorisation process to access prospective data for law enforcement agencies should be equivalent to the existing process under section 39 of the* Surveillance Devices Act 2004*. They argue that the reporting obligations should also be the same, which would require amendment to proposed section 180 of the Bill. What is your response?*

The process for applying for an authorisation to access prospective information is generally equivalent to the process that applies to the application for a tracking device authorisation pursuant to section 39 of the *Surveillance Device Act 2004* (the SD Act).

An authorisation may only be granted by an 'authorised officer' which is defined as the head of the agency, a deputy head or a person holding a management position. Further, an authorisation may only be granted to assist in the investigation of an offence punishable by imprisonment for at least 3 years. This is equivalent to the authorisation level and threshold for a tracking device authorisation contained in the SD Act. Authorisations for prospective information may be valid for a period of up to 45 days where as a tracking device authorisation can only be valid for a period of up to 90 days.

The contents of an application for an authorisation will be determined by the Communications Access Co-ordinator. These requirements have not yet been determined.

Law enforcement agencies will be subject to greater reporting requirements than currently exist given the requirement to provide annual statistics on the number of authorisations obtained. Prospective information will provide different information to tracking devices. Tracking device authorisations only provide actual location

information to the agency whereas prospective information authorisations provide subscriber details, numbers called, duration of calls and in some cases the general geographic location of the phone when requested by the agency.

Given the difference between the information to be obtained, the Department considers that the reporting requirements in the Bill are appropriate.

*27. The Law Council feels that warrantless access to tracking devices for ASIO is contrary to section 26A of the ASIO Act, where a warrant under 26B or C can only be issued by the Minister. They also argue that there should an extension of the prohibition of secondary disclosure to ASIO. What is your response to these suggestions?*

A tracking device is defined in the ASIO Act as:

> A device or substance that, when applied to an object, enables a person to track the object or a person using or wearing the object.

Given that access to prospective telecommunications data does not involve applying a substance or a device to an object, it is the Department's view that a warrant issued by the Minister is not available to ASIO for the use of telecommunications data. This is consistent with the policy rationale behind the warrant provisions which requires a warrant where the investigative method necessitates a trespass against the person. Telecommunications data does not involve such a trespass.

The Department considers that ASIO should remain exempt from the secondary disclosure prohibition. Inclusion of ASIO in the prohibition could disclose operational capabilities.

The Department is also of the view that the wide review and inspection powers are a sufficient accountability mechanism in relation to the secondary disclosure of information

***Threshold tests for privacy considerations – proposed sections 180(5) and 189(4)(c)***

*28. Several submissions felt the references to privacy considerations in these sections need to be strengthened or supplemented with further operational guidelines. The Law Council feels the sections should be rephrased in terms of a test – where the benefit to the criminal investigation must substantially outweigh the privacy harm. The OPC thought that practical guidance should be offered to decision-makers in the form of checklists, etc. What is your response to these concerns?*

The provisions relating to the consideration of a target's privacy mirror those provisions which already exist in relation to the issuing of telecommunications interception and stored communications warrants. Given that these tests exist in relation to the actual content of a communication, it would appear that the explicit reference to considering privacy is a valid accountability mechanism in relation to access to telecommunications data.

In relation to providing assistance to decision-makers, the Department will continue to provide advice to stakeholders on any concerns or queries which they may have in the operation of the proposed Bill.

***Form of authorisations***

*29. Both the Law Council and the WA Police are concerned with the form of authorisations to be decided by the CAC under proposed subsection 183(2). What requirements if any are likely to be imposed by a determination under this provision?*

As was the case with the creation of telecommunications interception and stored communications warrants, the Department aims to develop a specific form of authorisation prior to the commencement of the Bill should it pass. The Department will ensure that it consults with all relevant bodies in determining requirements for an authorisation. These may include the telecommunications service for which data is to be accessed, the agency authorising the access, the name of the authorised officer authorising the access and a declaration that the authorising officer has taken into account all relevant considerations.

***Call Charge Records***

*30. Several of the submissions from State Police have noted that they would like to use call charge records obtained for law enforcement purposes for the secondary purpose of police disciplinary proceedings. Is this a reasonable amendment in your view?*

The Department has received competing requests about the extent to which telecommunications data can be used in relation to police disciplinary proceedings. The Department understands the desire of State Police agencies to demonstrate a commitment to the accountability of its Officers.

However, other bodies such as the Police Federation of Australia have expressed concern that the operating legislation under which they work leaves them in a position where many disciplinary proceedings, despite being administrative in nature can be investigated with telecommunications data which has been accessed by way of a secondary disclosure.

The TIA Act has a strong focus on individual privacy and it is the Department's view that allowing secondary disclosure only when the conduct being investigated attracts a criminal or pecuniary penalty, or where it protects the public revenue, is an appropriate balance between the above positions.

***Testing***

*31. The IGIS has questioned whether the coverage of testing network infrastructure is wide enough. What is your response to this?*

And

*32. Schedule 2 items 11 and 12 would expand the current exemption for the AFP to cover Commonwealth agencies (AFP, ACLEI and ACC), security authorities (ASIO, Defence, DFAT) and eligible authorities of a State (police forces and integrity commissions), all of which are defined in subsection 5(1). Why was this deemed necessary? Why are other Commonwealth agencies excluded?*

The Department recognises that a number of agencies across the public and private sector need to ensure the security of their networks. The Department is also aware that changing technologies have made the existing provisions of the TIA Act

increasingly at variance with the ways in which networks operate. As such, some legitimate network protection activities may result in technical breaches of the TIA Act.

The current and proposed exemptions represent an interim measure to provide protection for those agencies that require the highest levels of network security. The Department is currently working on a permanent solution, which needs to take into consideration developing technologies and threats, systems administration procedures and workplace privacy.

33. *The OPC has made 5 major recommendations on this Bill in submission no. 19. What is the AGD response to the recommendations that:*

*a. there may be a role for IGIS in assisting exempt agencies to develop and implement standards for handling personal information;*

As noted in relation to Question 21, the IGIS is an independent statutory officer with extensive powers to scrutinise actions of the intelligence and security agencies. The IGIS has access to all of ASIO's records and staff and may enter the agency premises at any time. The IGIS regularly undertakes compliance inspections of ASIO's records and reports on his findings in the IGIS Annual Report.

Accordingly, the Department considers that the IGIS already has the necessary jurisdiction to oversee ASIO's handling of personal information.

*b. the Bill include provisions to place positive obligations on law enforcement agencies to destroy irrelevant material containing personal information collected through voluntary disclosure;*

See answer to Question 24 above.

Additionally, the limitation on the use of information under section 181 means that information can only be used in relation to a lawful disclosure of telecommunications data, and that the use is in connection with that lawful disclosure. This means that telecommunications data which is irrelevant to a criminal investigation cannot be lawfully used. It is our view that this provision provides an equal protection as the need to destroy irrelevant information.

*c. certifying officers authorised to approve access to prospective information should be provided with practical guidance to enable them to discern when the privacy of any person or persons is likely to be interfered with (subclause 180(5));*

The Department is of the view that the privacy issues which must be considered by certifying officers are an important accountability mechanism within the Bill. It is also important to note that there will be varying circumstances in which proposed section 180 will be used. It is therefore the view of the Department that it is happy to provide guidance to all agencies which can use the provisions of section 180, however general guidelines would be of such a vague nature as to not provide practical assistance.

*d. in relation to interception capability activities (clause 189):*

- *a note be appended to subclause 189(4), or comment made in the explanatory memorandum, which provides guidance about how the privacy of telecommunications users will be taken into account when making a Determination; and / or*
- *the inclusion of appropriate consultation mechanisms in this process including consultation with the Privacy Commissioner; and*

Carriers and carriage service providers require clear timeframes to effectively establish a new telecommunications service. A mandated consultation period may undermine the capacity of a determination under section 189 to effectively respond to this need. To find an appropriate balance to this requirement for expediency, the provisions of section 189 provide the Minister with considerations that must be taken into account prior to a determination being made.

In addition, it is noted that the Minister administering the TIA Act (the Attorney-General) is also the Minister who administers the *Privacy Act 1988*. It is the view of the Department that this allows privacy issues to be given detailed consideration when examined in the interception framework.

*e. the operation of the TIA Act should be subject to an independent review at least every five years.*

See answer to Question 4 above.

**The following information is provided by the Department in response to questions taken on notice by officers at the public hearing in Canberra, Monday 16 July 2007**

*1. Matters raised in the submissions from the Police Federation of Australia and Electronic Frontiers of Australia.*

Police Federation of Australia

See answer to Question 14 above.

Electronic Frontiers Australia

The Department has addressed a number of issues raised in the Electronic Frontiers Australia's submission in evidence given at the hearing and in the Questions on Notice received from the Committee.

*2. Government response to the Report of the Review of the Regulation of Access to Communications (the Blunn Review)*

The Government has not released a formal response to the Report. However, many of the recommendations of the Blunn review are either of an administrative nature, have been implemented in the *Telecommunications (Interception) Amendment Act 2006* or are contained in the current Bill. The Government is yet to make decisions on the remaining recommendations.

A table indicating the status of recommendations from the Blunn review is at Attachment A.

*3. Schedule 2 to the Bill*

A table outlining the provisions of Schedule 2 to the Bill that are not associated with the recommendations from the Blunn Review is at Attachment B.

*4. Late submissions received from the Law Council of Australia, Western Australian Police and the Office of the Privacy Commissioner.*

The Department has reviewed these submissions and has no additional comments to make.

The issue concerning the destruction of records raised by the OPC has been responded to at Questions 24 and 33b of the Questions on Notice.

*5. The inclusion of Crimtrac as an enforcement agency*

The *Telecommunications Act 1997* currently provides for a body or organisation responsible to the Australasian Police Ministers' Council for the facilitation of national law enforcement support; including the National Exchange of Police Information access to telecommunications data.

In transferring provisions from the Telecommunications Act to the TIA Act, continued access for all agencies has been maintained while current requirements for access to this information are investigated. Discussions with Crimtrac are continuing.

Crimtrac manages a number of advanced information systems and accesses telecommunications information on behalf of law enforcement agencies across Australia.

The inclusion of Crimtrac in the definition of an enforcement agency in the TIA Act will not in itself allow Crimtrac to access stored communications. Stored communications may only be accessed by an enforcement agency where they have satisfied an issuing authority that the information that would be obtained would likely assist in connection with the requesting agencies investigation of a serious contravention, being an offence punishable by imprisonment for a maximum period of 3 years.

As Crimtrac's functions do not include the investigation of any offences, they will not be eligible to be issued with a stored communications warrant.