CHAPTER 3

KEY ISSUES

3.1 This chapter examines the main issues and concerns raised in the course of the committee's inquiry. Submissions to the inquiry were generally favourable to the Bill, especially the desirability of a single comprehensive legislative regime dealing with access to telecommunications information.[1]

3.2 Two submissions, from Electronic Frontiers Australia (EFA) and the Australian Privacy Foundation (APF), suggested that the Bill is so flawed that it should not be passed. These organisations focused on privacy implications of the new regime for access to telecommunications data. Several organisations recommended the Bill be passed with minor amendments, many of which involve limiting the language of various definitions in the Bill.

3.3 The main issues raised include:

- the definition of key terms such as 'enforcement agency' in the Bill;
- the lack of a definition of 'telecommunications data';
- privacy concerns, particularly in relation to access to prospective telecommunications data and the impact of the secondary disclosure provisions on police officers;
- the obligations on telecommunications companies;
- concerns about whether the amendments meet the need to protect critical infrastructure; and
- the mechanisms for reporting, oversight and review.

Consultation

3.4 The amendments in the Bill were the subject of a consultation process run by the Attorney-General's Department.[2] An officer of the Department outlined the consultation undertaken:

> [W]e developed the draft legislation in close consultation with Commonwealth government agencies. That was an internal consultation process. We released the exposure draft of the bill in February [2007] and we received 32 submissions addressing the various provisions. To follow up on that we also had a number of meetings and conversations with

1 See, for example, Optus, *Submission 2;* Department of Defence, *Submission 3*; Communications Alliance Ltd, *Submission 18*, p. 1; Tasmania Police, *Submission 23*, p. 2.

2 Full details about the consultation process are given by the Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, pp 4-8.

> industry groups and various submitters to work through some of the issues that they raised. Quite a few of the issues that they have raised have resulted in amendments between the exposure draft and the [bill] that was subsequently introduced.[3]

3.5 The Office of the Privacy Commissioner (OPC) noted that 'a number of the issues raised in our previous submission have been addressed in the Bill and Explanatory Memorandum'.[4] Similarly, Mr Chris Althaus of the Australian Mobile Telecommunications Association (AMTA) commented at the hearing that:

> There was over an extended period a high degree of interaction with the industry. We had a number of concerns particularly in relation to standards and powers within the exposure draft. We were able to put an argument forward, the government listened to that, and that was an important amendment in our view. In many respects it was the most important amendment that came forward.[5]

Definitions

Definition of 'enforcement agency'

3.6 EFA submitted that CrimTrac should be deleted from the definition of 'enforcement agency' on the basis that it is not a criminal law enforcement agency or an agency that conducts investigations.[6] EFA was also concerned that the inclusion of CrimTrac in the definition of 'enforcement agency' would give CrimTrac access to stored communications warrants under section 110 of the TIA Act.[7]

3.7 The Law Council of Australia (Law Council) expressed concern at the inclusion of paragraph (k) in the proposed definitions of 'enforcement agency' and 'criminal law-enforcement agency'. This provision allows an authority established under a Commonwealth, state or territory law to be added to these definitions by regulation. The Law Council was particularly concerned that this would allow delegated legislation to expand the range of agencies which will be able to authorise access to prospective telecommunications data:

> 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

---

3 *Committee Hansard*, 16 July 2007, p. 30.

4 *Submission 19*, p. 2.

5 *Committee Hansard*, 16 July 2007, p. 18. See also Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, pp 4-5.

6 *Committee Hansard*, 16 July 2007, p. 10. See also Law Council of Australia, *Submission 20*, p. 14.

7 *Submission 6a*, p. 5.

for why the efficient operation of the TIA Act requires the sort of flexibility afforded the Executive under paragraph (k).[8]

Departmental response

3.8 In relation to the inclusion of CrimTrac in the definition of 'enforcement agency', an officer of the Department advised:

> [CrimTrac] are an enforcement agency in terms of telecommunications data. That is an existing provision under the Telecommunications Act…At this stage we have transferred over the agencies provided within the definition of 'enforcement agency' under the Telecommunications Act and we are looking to see whether or not it is appropriate that they continue to be within that definition. Until such time as we can actually establish that it is not appropriate, we have not removed them.[9]

3.9 The Department explained further:

> 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.[10]

3.10 On the issue of the power to expand the definitions of 'enforcement agency' and 'criminal law-enforcement agency' by regulation, the Department responded:

> 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.[11]

---

8 *Submission 20,* p. 13.

9 *Committee Hansard,* 16 July 2007, p. 10.

10 *Answers to questions on notice*, 24 July 2007, p. 22.

11 *Answers to questions on notice*, 24 July 2007, p. 10.

Meaning of 'telecommunications data'

3.11 There is no definition of 'telecommunications data' in the Bill. Instead, proposed section 172 prevents the provisions which permit the disclosure of telecommunications data from applying to the 'contents or substance of a communication'. Subject to this limitation, the provisions in Chapter 4 then authorise access to 'information or a document'.

3.12 In its comments on the Exposure Draft of the Bill, OPC suggested that the distinctions between 'information or a document' and 'contents or substance' may be difficult to discern in some cases and called for further clarification, given that the prohibitions against disclosure in the TIA Act attract a serious penalty.[12] OPC welcomed the inclusion in the EM of material to clarify the distinction between call data and the content of a communication.[13]

3.13 However, the APF and EFA felt that these changes did not go far enough and expressed particular concern about the potential to access information about web browsing and chat room sessions, and email header data as telecommunications data.[14] APF argued:

> We are very disappointed that such a fundamental revision of the relevant provisions has missed the opportunity to more clearly define what is meant by key terms such as 'telecommunications data' and 'content or substance'. This creates unacceptable ambiguity and uncertainty about the 'reach' of the various powers and protections. It also leaves open the possibility that very sensitive information such as mobile phone location data, email message headers and various Internet logs would not be considered 'substance or content' or stored 'communications', and would therefore be subject not to the TIAA warrant controls but to the much weaker protection applying to 'authorisations'…We submit that a much clearer legislative distinction between 'traffic data' and 'substance and content' is required.[15]

3.14 Similarly, EFA suggested that the distinction between the content or substance of a message and other data was particularly unclear in relation to email header data:

> In our view the subject line is part of the content of a message, but existing legislation is silent on this matter and it cannot be known whether the same view would be held by all carriers and enforcement agencies. Furthermore, email messages can carry significantly more…information in the header section than is equivalent to 'traffic information' associated with telephone

---

12 Office of the Privacy Commissioner, *Submission on Exposure Draft of the Telecommunications (Interception and Access) Amendment Bill 2007*, February 2007, at http://www.privacy.gov.au/publications/subtel0207.html (accessed 1 July 2007).

13 *Submission 19*, p. 2.

14 *Submission 6*, pp 9-12; *Submission 17*, p. 3.

15 *Submission 17*, p. 3.

> calls. For example, some (probably most) email programs enable the end-user to create their own special header fields in outgoing messages, in which they can place any information they wish.[16]

3.15 As a result, EFA suggested that clarification of the distinction between data and content in relation to email messages should be included in the Bill.[17]

3.16 EFA further argued that the Bill should be amended so that access to information regarding Internet sessions would only be permitted under a stored communications warrant.[18] EFA submitted that the data which may be captured in relation to Internet sessions is qualitatively different to telecommunications data about telephone calls and email messages:

> 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.[19]

Departmental response

3.17 The Department advised that there was no intention to insert a definition of 'telecommunications data' into the Bill and explained:

> Our concern about defining what technology and call associated data may be now [is that the definition] might be redundant in 12 months time. Essentially we rely on the premise that the contents and substance of a communication are protected and are only accessible under a TIA warrant, an interception warrant or a stored communication warrant, and it is the other information that attaches to a communication but does not disclose the contents or the substance of that communication that is the associated data. One of the points of bringing this all into one piece of legislation is the hope that by having the three limbs together it will be clearer when advising law enforcement and the carriers on what exactly is content and what is call associated data as new technologies come into place.[20]

---

16 *Submission 6*, p. 9.

17 *Submission 6*, pp 9-10. The Department has agreed to review the EM to remove any ambiguity. See Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, p. 13.

18 *Submission 6*, p. 12.

19 *Submission 6*, p. 4.

20 *Committee Hansard*, 16 July 2007, p. 22.

3.18 The EM states that the subject line of an email or details of Internet sessions are not captured as 'telecommunications data'.[21] At the hearing, an officer of the Department clarified what information would be captured as telecommunications data in relation to web browsing:

> In relation to getting call-associated data regarding an IP [Internet Protocol] address that can identify a web page, that is not content because all it does is tell a law enforcement agency that a certain target went to a certain website. It does not tell them any other details. It does not tell them that they then went into their bookings online or via their travel agent or that they downloaded particular information. It does not give them any knowledge of the substance as to why they were on that web page. URLs [Uniform Resource Locators] are a little different because they will then point out the continuum of where the person actually went to.[22]

3.19 The Department went on to argue that URL data was equivalent to a telephone number in terms of the information provided:

> With regard to web URLs—or URIs [Uniform Resource Identifiers] —and how an apparatus finds that on the Internet, I will go back to the analogy of when we used to make telephone calls; if we had call charge records we would have a list of numbers that a person called but it does not show content...If an officer wants to phone those numbers and find out what they are they could ring them systematically. It is the same with a computer. When they go and click that button to search that URL, it is the same thing.[23]

3.20 The Department also responded to EFA's concerns that email header data may be captured as telecommunications data:

> 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'.[24]

---

21 p. 8.

22 *Committee Hansard*, 16 July 2007, p. 31.

23 *Committee Hansard*, 16 July 2007, p. 31.

24 Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, pp 10-11. The EFA disputes the Department's interpretation of RFC 2822: see *Submission 6b*.

Privacy concerns

3.21 Several submissions raised concerns regarding the impact the Bill would have on privacy, in particular the provisions relating to access to prospective telecommunications data and to secondary disclosure of data.

Access to prospective telecommunications data

3.22 EFA expressed concerns about the potential use of real time access to telecommunications data to track individuals using data obtained from mobile telephones. EFA stated, in relation to prospective data, that:

> New technologies such as Assisted GPS, reportedly expected to be introduced in Australia by some carriers in 2007 or 2008, will greatly improve the accuracy of mobile phone location information. Access to 'prospective' location information enables not only identifying/tracking location but potentially real world, real time, surveillance of a tracked individual's activities.[25]

3.23 EFA therefore submitted that access to prospective mobile telephone data should be subject to more stringent control than authorisation by certain officers in ASIO or a criminal-law enforcement agency:

> [W]e are very concerned that this bill will enable tracking of people via mobile phone location information without a warrant, which is basically further extending the definition of 'telecommunications data'…This bill appears to have the specific purpose of allowing law enforcement agencies to use a person's own tracking device that they carry with them all of the time. Because it is a device that can be used to track a person without the need to covertly install a tracking device on a person's property or body, we believe that there is considerably more potential for misuse of these new powers. We are strongly of the view that for that kind of information to be collected in near real time, because it will enable physical visual of track people, a warrant should be required similar to the existing surveillance device warrants in the Commonwealth and the various states, or with similar conditions attached as the stored communications warrants.[26]

3.24 The Law Council acknowledged that the Bill places greater controls on access to prospective telecommunications data (under proposed sections 176 and 180) than access to existing data (under proposed sections 175, 178 and 179). However, the Law Council considered that these controls do not go far enough.[27] The Law Council also argued that criminal law-enforcement agencies should require a

---

25 *Submission 6*, p. 4.

26 *Committee Hansard*, 16 July 2007, p. 9. See also New South Wales Council for Civil Liberties, *Submission 10*, p. 3; Australian Privacy Foundation, *Submission 17*, p. 4.

27 *Submission 20*, p. 6.

warrant in order to access prospective telecommunications data and thus use a person's mobile telephone 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. 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.
>
> 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.[28]

3.25 The Queensland Council for Civil Liberties also expressed concern that the Bill would allow mobile telephone location information to be disclosed under a written authorisation for a period of 45 or 90 days without the need to obtain a warrant.[29]

Departmental response

3.26 The Department noted that the Telecommunications Act already provides for enforcement agencies to access prospective telecommunications data:

> Access to prospective data already exists under the current regime. In moving it over to the TIA act, we have acknowledged that there are two accesses under section 282 of the act—that is, historical data and information in real time.[30]

3.27 In response to concerns about the privacy implications of access to prospective data from mobile telephones, the Department argued that the new regime imposes more stringent requirements for access to prospective data:

> From our perspective that is addressed by the fact that we have acknowledged that there is potentially a greater breach of privacy if a person can access prospective data, and that is why we have separated it out from historical data. We have placed a time limitation on it. We have also limited the agencies that can access this information to criminal law

28 *Submission 20*, pp 6-7.

29 *Submission 8*, p. 2.

30 *Committee Hansard*, 16 July 2007, p. 23.

> enforcement and national security agencies, and we have made it an offence that is punishable by three years, which is consistent with the surveillance devices legislation.[31]

Secondary disclosure provisions

3.28 The Police Federation of Australia (Police Federation) held concerns regarding how proposed section 182 may impact on the privacy rights of police officers, especially those involved in disciplinary proceedings.[32] Proposed section 182 would allow the secondary disclosure and use of telecommunications data where the disclosure is reasonably necessary 'for the enforcement of a law imposing a pecuniary penalty'. At the hearing, Mr Mark Burgess of the Police Federation explained that:

> the disciplinary offences applicable to most police jurisdictions are found within state and territory legislation and have provisions for pecuniary penalties by way of fines even for very minor matters.[33]

3.29 Mr Burgess gave further evidence that:

> We are concerned that the bill will give the ability to disclose information, as limited as it might be, which will therefore allow people to undertake fishing expeditions for further information that they might think they can gather, and when they might not have been aware of any of this in the first place. This is not about preventing appropriate use of this legislation or this bill to target police officers undertaking criminal or corrupt activities. Our concern centres around the prospect of it being used in respect of what all of us in this room would consider to be minor disciplinary issues. Because the relevant legislation that underpins those disciplinary issues has provisions for monetary penalties, they will be picked up.[34]

3.30 The Police Federation argued that the definition of 'pecuniary penalty' in the Bill should be narrowed or the reference deleted. In the alternative, the Police Federation submitted that the secondary disclosure provision should exempt police disciplinary proceedings.[35]

3.31 On the other hand, the NSW Ombudsman argued that the current restrictions on secondary disclosure are too narrow and that secondary disclosure of telecommunications data to the Ombudsman to support its role in investigating police misconduct should be permitted.[36] The Western Australian Police also supported

---

31 *Committee Hansard*, 16 July 2007, p. 24.

32 *Submission 4*, pp 1-3.

33 *Committee Hansard*, 16 July 2007, p. 2.

34 *Committee Hansard*, 16 July 2007, p. 3.

35 *Submission 4*, pp 2-3.

36 *Submission 7*, pp 1-2.

allowing secondary disclosure of telecommunications data, such as call charge records, for the purpose of police disciplinary proceedings.[37]

Government response

3.32 The Police Federation submitted correspondence from the Attorney-General which explained that the bill 'permits the secondary disclosure of information to an agency in circumstances where the receiving agency would itself have been able to access the information directly from the carrier.'[38] The Attorney-General also noted that the meaning of 'pecuniary penalty' 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 a financial impact, such as for example, a demotion'.[39]

3.33 The Department gave further evidence regarding the difficulties involved in excluding police disciplinary proceedings which impose a pecuniary penalty from the operation of proposed section 182:

> In general terms it would not be appropriate to exclude pecuniary penalties overall. Obviously under some of the individual state and territory police acts some of the pecuniary penalties that would trigger the secondary disclosure provisions would be quite serious. Given that 'pecuniary penalty' is a fairly broad term, the alternative would be to try to insert more detailed definitions that relate and encompass all those different state and territory police acts. Before we did that we would need to consult closely with each of the state and territory police commissioners. It should also be said that, because the definitions in question that are giving the Police Federation trouble are in the state and territory legislation, our view is that it is probably better that they deal with it as a matter under the state employment legislation.[40]

Consideration of privacy implications

3.34 Privacy NSW commented favourably on the requirement in proposed 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 telecommunications data.[41] Privacy NSW suggested proscribing (by way of regulation or similar) a requirement to have each enforcement agency (to whom

37 *Submission 21*, p. 2.

38 *Submission 4*, attachment, p. 2.

39 *Submission 4*, attachment, p. 2.

40 *Committee Hansard*, 16 July 2007, pp 30-31. See further Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, pp 11-12.

41 *Submission 16*, p. 1.

authorising officers belong) develop guidelines on how the privacy implications of an authorisation should be considered and documented.[42]

3.35 OPC made a similar recommendation that authorised officers be provided with practical guidance, in the form of a note to the Bill or detail in the EM, to assist them in discharging the obligation in proposed subsection 180(5).[43]

3.36 Privacy NSW and OPC also made recommendations regarding proposed paragraph 189(4)(c) which provides that the Minister, before making determinations in relation to interception capabilities, must take into account the privacy of the users of telecommunications systems.[44] In particular, OPC suggested:

> …the inclusion of a note to the clause, or in the explanatory memorandum, which provides guidance about how the privacy of telecommunications users will be taken into account in the making of the determination.[45]

3.37 In the same vein, NSW Council for Civil Liberties welcomed the inclusion of privacy as a consideration in proposed sections 180, 183 and 189 but suggested that there should be 'further elaboration of this requirement in the Bill by way of substantive requirements for protection of privacy.'[46]

Departmental response

3.38 The Department noted that the issue of providing further guidance on the consideration of interference with privacy under proposed subsection 180(5) had been raised during consultation on the Exposure Draft and advised that:

> 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 [Communications Access Coordinator] may wish to address in the procedural requirements provided for in new section 183.[47]

---

42 *Submission 16*, p. 1.

43 *Submission 19*, p. 2.

44 *Submission 16*, p. 1; *Submission 19*, p. 4.

45 *Submission 19*, p. 4.

46 *Submission 10*, p. 2.

47 *Answers to questions on notice*, 24 July 2007, p. 5.

Destruction of data

3.39 Proposed sections 174 and 177 deal with voluntary disclosures of telecommunications data to ASIO and enforcement agencies by employees of a carrier or carriage service provider. OPC suggested that these provisions include:

> …positive obligations on law enforcement agencies to destroy irrelevant material containing personal information collected under these provisions together with information which is no longer needed by such law enforcement agencies and to do so in a timely manner.[48]

Departmental response

3.40 The Department advised in relation to this suggestion that:

> The Government will consider this recommendation, but notes reservations about the need for such an amendment. [49]

3.41 In particular, the Department suggested an amendment may not be required due to the limitation that proposed section 181 would place on the *use* of data lawfully disclosed under the TIA Act:

> [T]he 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.[50]

Obligations on carriers and carriage service providers

3.42 While submissions from the telecommunications industry generally supported the Bill, they suggested minor amendments to the provisions relating to obligations on telecommunications companies.

Communications Access Coordinator

3.43 AMTA suggested amendments to proposed section 6R to require the CAC to act in accordance with the objects and regulatory policy of the Telecommunications Act in the performance of his or her duties under Chapter 5 of the TIA Act.[51] Mr Chris Althaus of AMTA noted:

---

48 *Submission 19*, p. 3.

49 *Answers to questions on notice*, 24 July 2007, p. 16.

50 *Answers to questions on notice*, 24 July 2007, p. 19.

51 *Submission 5*, p. 2.

> The Communications Access Coordinator role seems to be one that is particularly pivotal and we would like to see the objectives of the Telecommunications Act picked up by the CAC…[52]

3.44 Vodaphone also considered that the replacement of the existing provisions regarding 'agency coordinator' in the Telecommunications Act with the new provisions establishing the CAC in the TIA Act resulted in:

> …a lack of guidance afforded to the role of Communications Access Co-ordinator in the conduct of its functions where previously there existed at least some degree of clarity. This arises as a result of the removal of provisions under the *Telecommunications Act 1997* that mandated that certain objects of the legislation were to be borne into account in the exercise of these Co-ordinator's functions.[53]

Departmental response

3.45 An officer of the Department gave evidence that the amendment proposed by AMTA to the definition of the CAC was unnecessary:

> The objects of the Telecommunications Act are picked up under several of the powers of the Communications Access Coordinator…The role of the CAC is to make decisions on behalf of law enforcement—national security—in relation to particular things, so we are not sure that it would add anything. The definition, except for the change of the name from the agency coordinator, is exactly as it has been since 1997 and it has worked extremely successfully.[54]

Delivery points

3.46 AMTA and Telstra expressed concerns regarding the factors ACMA will take into account when determining delivery points under proposed subsection 188(6).[55] AMTA explained that:

> …meeting the Delivery Capability requirements often involves the installation of specialised equipment for this purpose. In practical terms, the location of a delivery point will be affected by the physical location of equipment performing the Delivery Capability function. Therefore, the factors to be considered in determining Delivery Points should also take account of the location of any equipment performing Delivery Capability functions.[56]

---

52 *Committee Hansard*, 16 July 2007, p. 13.

53 *Submission 11*, p. 2.

54 *Committee Hansard*, 16 July 2007, p. 28.

55 *Submission 5*, p. 6; *Submission 9*, p. 1.

56 *Submission 5*, p. 6.

Departmental response

3.47 In evidence to the committee, the Department noted that proposed section 188 did not alter the existing arrangements under the Telecommunications Act in relation to delivery points. The Department also explained that, under proposed section 188, carriers will nominate delivery points in the first instance.[57] It is only where a carrier and an interception agency cannot agree on a delivery point that ACMA will be required to make a determination under proposed subsection 180(5).

Interception capabilities

3.48 AMTA and Telstra objected to the definition of 'interception capability' in proposed subsection 187(2).[58] In particular, AMTA was concerned that:

> …the proposed definition includes any equipment connected to a telecommunications network. Provision of services in an Internet environment involves use of a variety of separate components that are clearly defined in the *Telecommunications Act 1997*, including customer equipment, carriage services, that is, the carrying of Internet 'packets' across networks and Internet applications and content services, such as instant messaging and web hosting. For the most part Internet applications, content services and customer equipment can be independent of the Carrier or CSP [Carriage Service Provider].[59]

3.49 AMTA suggested changes to the definition in proposed subsection 187(2) to provide that interception capability is not required in relation to 'customer equipment', or equipment supplying a 'content service', as these terms are defined in the Telecommunications Act.[60]

3.50 Vodaphone also submitted that:

> Some clarification may be required in the area of converged services with the apparent grouping and classification of Internet content services and applications onto the existing responsibilities of Carriers and Carriage Service Providers. These obligations appear to be imposed without adequate consideration given to the nature of proprietary applications and attention to the inability of Carriers to apply operational control over such matters as third party equipment.[61]

---

57 *Committee Hansard*, 16 July 2007, p. 27.

58 *Submission 5*, pp 2-3; *Submission 9*, p. 4.

59 *Submission 5*, pp 2-3.

60 *Submission 5*, p. 3.

61 *Submission 11*, p. 2.

Departmental response

3.51 The Department explained that where equipment is not within the control of carriers they will not have an obligation to provide interception capability. However, an officer of the Department noted:

> AMTA were talking about customer premise equipment and they referred to the Telecommunications Act. Within the Telecommunications Act 'customer premise equipment' refers to the equipment that resides within the premise of the customer—for example, mainframes, network terminating units, routers and switches. They gave examples of how in the new technology age these are becoming less in control of the carrier. In our view in some cases in the industry they manage or remotely manage those routers, switches or mainframes. Therefore, we believe with regard to the definition under the act that the physical location does not dictate whether or not the equipment is under the control of the carrier.[62]

Interception capability plans

3.52 Proposed section 196 requires carriers to develop interception capability plans (ICP) and proposed section 195 sets out matters that must be included in the plan. AMTA submitted that proposed section 195:

> …significantly expands the factors that must be included in an Interception Capability Plan to include 'or a change in marketing or pricing of services'. AMTA is concerned that this section 195 will place a significant burden on carriers and CSPs [carriage service providers] to submit updated plans to the CAC each time a price change is made or marketing campaign is launched for each product service.[63]

3.53 Proposed paragraph 195(2)(f) and proposed subsection 195(4) would permit the Minister to determine additional matters that must be dealt with by an interception capability plan. Telstra expressed concern that this may allow the Ministerial determination to expand the scope of a carrier's interception capability obligations. It suggested that proposed subsection 195(4) should be amended to clarify that any matters specified by the Minister to be included in the interception capability plan should only relate to matters relevant to a carrier's interception capability obligations.[64]

Departmental response

3.54 In response to a question on notice, the Department rejected AMTA's view that proposed section 195 significantly expanded the matters that must be addressed in an interception capability plan:

---

62 *Committee Hansard*, 16 July 2007, p. 29.

63 *Submission 5*, p. 4. See also *Committee Hansard*, 16 July 2007, p. 16.

64 *Submission 9*, p. 4.

> 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.[65]

3.55 In relation to Telstra's concern that proposed subsection 195(4) would permit the Minister to expand the matters to be dealt with by an interception capability plan beyond matters relevant to a carrier's interception capability obligations, the Department advised that:

> 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.[66]

Exemptions

3.56 The Communications Access Coordinator (CAC) may grant exemptions to interception capability obligations under proposed section 192. Under proposed subsection 192(5), a carrier will be deemed to have an exemption where the carrier has applied in writing to the CAC and the CAC has not communicated a decision on the exemption application within 60 days of the application. Proposed subsection 192(6) provides that a deemed exemption only has effect until the CAC communicates to the carrier a decision on the exemption application.

3.57 Mr Michael Ryan of Telstra explained industry concerns with the operation of deemed exemptions:

> [F]rom our point of view the CAC has 60 days to consider an exemption application, and it is deemed after 60 days that you have got an exemption. The problem is that CAC can come back and say you no longer have that exemption, which then leaves us in a state of uncertainty as to what we do with those applications…It makes it very uncertain in terms of delivering advanced services to customers if there is no time line or dead end to the deemed period.[67]

3.58 AMTA argued that there should be a time limit of 180 days on the refusal of an exemption by the CAC under proposed subsection 192(6) unless the CAC could

---

65 *Answers to questions on notice*, 24 July 2007, p. 9.

66 *Answers to questions on notice*, 24 July 2007, p. 6.

67 *Committee Hansard*, 16 July 2007, p. 16.

establish that a demonstrated agency need for interception exists. Alternatively, AMTA suggested that this provision should be repealed.[68]

Departmental response

3.59 The Department advised the committee that, in practice, this issue was unlikely to arise as in the last two years no exemption application had required more than 60 days to reach a decision.[69] The Department also noted that:

> The situation is such that when any application for exemption is made, if it is a complex one—if there is a potential that an exemption will not be granted—we engage immediately with the provider so that there will be no potential surprises. We try to work with them to come up with a solution if we believe that they strongly need interception capability…[W]e seek that the providers ask for an exemption from their capability prior to the rollout of that service, because we do not want to slow down the rollout of services...We do not ask them to retrofit; we ask them to talk to us in advance of rolling out a service.[70]

Ministerial determinations

3.60 Telstra expressed concern about the Minister's power to make determinations in relation to interception capability under proposed section 189 and, in particular, the range of factors the Minister would be required to consider before making a determination. In response to a question on notice, Telstra stated that:

> …the section should be broadened to require the Minister to take into account the effect of the determination on the ability for new and innovative products to be introduced into the Australian market, as well as on existing products and services in the market (which includes the costs implications of making existing products/services compliant with the subsequent determination).[71]

3.61 Telstra explained further:

> In terms of new and innovative products and services, there may be various issues which make it extremely difficult or impossible to provide an interception capability. For instance, the Minister may issue a determination which requires industry to intercept a new or innovative product/service which may be hosted overseas where the overseas product vendor is unable to provide interception capability due to jurisdictional and/or technology

68 *Submission 5*, pp 3-4. See also Telstra, *Submission 9*, p. 3.

69 *Committee Hansard*, 16 July 2007, p. 30. See also Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, p. 6.

70 *Committee Hansard*, 16 July 2007, pp 29-30.

71 *Answers to questions on notice*, 24 July 2007, p. 1.

> constraints. In this scenario, it may result in the new and innovative product/service not being able to be made available in Australia.[72]

Departmental response

3.62 The Department noted in evidence to the committee that the Minister would be required to consider the objects of the Telecommunications Act in making determinations in relation interception capabilities.[73] The EM explains that the objects of the Telecommunications Act include:

> …the provision of a regulatory framework that promotes the long term interests of end-users of carriage services, or of services provided by means of carriage services; and the efficiency and international competitiveness of the Australian telecommunications industry.[74]

Other issues

Network protection

3.63 Subsection 5F(2) and 5G(2) of the TIA Act currently provide the AFP with exemptions for the purposes of network protection and enforcing professional standards. Schedule 2, Items 11 and 12 would expand the current exemptions for the AFP to cover Commonwealth agencies (AFP, 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). These provisions will enable those agencies to monitor inbound and outbound communications for the purpose of enforcing professional standards and protecting their networks without the risk of breaching the TIA Act.[75]

3.64 However, the Inspector-General of Intelligence and Security (the IGIS) questioned whether the coverage to allow network administrators in certain agencies to protect network infrastructure is wide enough:

> While one can well understand the need for adequate protection of the agencies which directly protect obvious national security interests (ie Australia's defence, security, international relations or law enforcement), the question also arises as to whether there is other network infrastructure the protection of which is also of particular importance to Australia's interests.[76]

---

72 *Answers to questions on notice,* 24 July 2007, p. 1.

73 *Committee Hansard*, 16 July 2007, p. 28.

74 EM, pp 18-19.

75 EM, p. 42.

76 *Submission 14*, pp 3-4. See also Premier of Western Australia, *Submission 25*, pp 1-2.

Departmental response

3.65 The Department responded to a question on notice on this issue:

> 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.[77]

Oversight

3.66 The IGIS noted there may be a role for his office in monitoring authorisations to access prospective telecommunications data by ASIO officers. The IGIS suggested that these authorisations should be examined as part of the IGIS inspection program:

> This would involve periodic visits by my staff during which they would review all of the authorisations granted in the preceding period to ensure that there was sufficient justification and that requirements imposed by the Communications Access Coordinator under the proposed section 183 were met.[78]

Departmental response

3.67 The Department agreed with this suggestion and argued that the existing jurisdiction of the IGIS under the *Inspector-General of Intelligence and Security Act 1986* would allow him to perform this role:

> 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.[79]

---

77 *Answers to questions on notice*, 24 July 2007, pp 18-19.

78 *Submission 14*, p. 2.

79 *Answers to questions on notice*, 24 July 2007, p. 15.

Review

3.68 On the issue of periodic reviews of the TIA Act, OPC submitted:

> …the operation of the Interception Act should be subject to overall independent review including key stakeholder and public consultation at least every five years.[80]

Departmental response

3.69 The Department did not accept that the TIA Act should be the subject of a mandatory statutory review process:

> 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.[81]

Committee view

3.70 The committee is satisfied that extensive consultation has occurred between the Department, the telecommunications industry, law enforcement and security agencies, and other interested parties. The committee, like many of these parties, welcomes the further implementation of recommendations made in the Blunn Review by the Bill, including establishment of a single comprehensive legislative regime dealing with access to telecommunications information.

3.71 The committee acknowledges that consultation between the government and the telecommunications industry is crucial to ensure that interception capabilities support the legitimate requirements of enforcement agencies without unduly impinging on the services provided by carriers and carriage service providers. While some submissions argued for formal requirements for consultation to be embedded in the Bill, the committee considers that continuation of the existing arrangements for consultation between government and industry are likely to be just as effective and considerably more flexible.

3.72 In the absence of any justification for the inclusion of CrimTrac in the definition of 'enforcement agency', the committee considers that CrimTrac should be removed from the definition. The inclusion of agencies in this definition provides

---

80 *Submission 19*, p. 6.

81 *Answers to questions on notice*, 24 July 2007, p. 5.

agencies with intrusive powers so the default position should be that agencies are excluded, unless a positive justification for their inclusion is forthcoming.

3.73 The committee believes that the suggestion that further guidance be provided to assist authorised officers in assessing the privacy implications of authorising access to prospective telecommunications data, as required by proposed subsection 180(5), is a constructive one. However, the committee is mindful of the Department's concerns that seeking to provide that guidance within the Bill is likely to be impractical given the range of circumstances confronting officers weighing these issues. The committee notes the Department's advice that privacy issues may be addressed through the determination of the CAC under proposed subsection 183(2) regarding the formal requirements for authorisations and notifications. The committee recommends that the CAC determination under that provision should address procedural requirements in relation to the consideration and documentation of privacy issues. In making this recommendation, the committee is mindful that proposed subsection 183(3) will require the CAC to consult with the Privacy Commissioner before making such a determination.

3.74 The committee supports the suggestion made by the IGIS that oversight of access to prospective telecommunication data by ASIO should form part of his regular inspection program. The committee notes advice from the Department that the existing powers of the IGIS would permit such inspections.

3.75 The Senate Legal and Constitutional Legislation Committee previously recommended an independent review of provisions inserted in the TIA Act by the Telecommunications (Interception) Amendment Bill 2006.[82] The committee believes that in light of the complexity of the legislation, its acknowledged impacts on privacy and the potential for significant changes in technology to substantially alter the reach and affect of provisions in the Act, an independent review of the TIA Act in the next five years is highly desirable. In particular, such a review would provide an opportunity to examine further the issues of:

- whether there is a need to define 'telecommunications data', or whether the distinction between 'content and substance' and other information and documents operates effectively;
- what impact further technological developments have on the operation of the TIA Act; and
- whether any of the obligations imposed on carriers and carriage service providers are unnecessarily hampering the efficient delivery of telecommunications services, including the introduction of new services.

3.76 The committee accepts the view of the government that it is unnecessary to amend the Bill to require such a review.

---

82 Senate Legal and Constitutional Legislation Committee, Provisions of the *Telecommunications (Interception) Amendment Bill 2006*, March 2006, Recommendation 25, p. 48.

Recommendation 1

3.77 The committee recommends that proposed paragraph 5(1)(m) of the Bill be deleted to remove CrimTrac from the definition of 'enforcement agency'.

Recommendation 2

3.78 The committee recommends that the determination of the Communications Access Coordinator under proposed subsection 183(2) address requirements for the consideration and documentation of privacy issues by authorised officers.

Recommendation 3

3.79 The committee recommends that the Inspector-General of Intelligence and Security incorporate into his regular inspection program oversight of the use of powers to obtain prospective telecommunications data by the Australian Security Intelligence Organisation.

Recommendation 4

3.80 The committee recommends that the Attorney-General's Department arrange for an independent review of the operation of the *Telecommunications (Interception and Access) Act 1979* within five years.

Recommendation 5

3.81 Subject to the preceding recommendations, the committee recommends that the Bill be passed.

Senator Guy Barnett
Chair