Parliament of Australia
Department of Parliamentary Services

Parliamentary Library
Information analysis and advice for the Parliament

BILLS DIGEST

3 August 2007, no. 10, 2007–08, ISSN 1328-8091

Telecommunications (Interception and Access) Amendment Bill 2007

Bronwen Jaggers
Law and Bills Digest Section

Contents

Telecommunications (Interception and Access) Amendment Bill 2007

Date introduced: 14 June 2007

House: House of Representatives

Portfolio: Attorney-General

Commencement: Sections 1 to 3 commence upon Royal Assent. Schedule 1, which contains the Bill's main amendments, commences on a date to be fixed by proclamation, or six months after Royal Assent. See the table in s. 2 of the Bill for a full list of commencement dates.

Links:
The relevant links to the Bill, Explanatory Memorandum and second reading speech can be accessed via BillsNet, which is at http://www.aph.gov.au/bills/. When Bills have been passed they can be found at ComLaw, which is at http://www.comlaw.gov.au/.

See also the Senate Inquiry into the Bill and the *Telecommunications (Interception and Access) Act 1979*, and *Telecommunications Act 1997* .

Purpose

The Bill proposes to transfer provisions in the *Telecommunications Act 1997* which regulate access to telecommunications data for national security and law enforcement purposes to the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). The Bill also proposes a new two-tier access regime for access to historic and 'prospective' telecommunications data. There are also some consequential amendments to other Acts.

Background

Basis of policy commitment

In response to increasingly sophisticated communication techniques by terrorists and terrorist suspects, such as storing emails in draft accounts but not sending them, swapping SIM cards and using others' telephones, in 2004 the government introduced interim legislation which allowed security and law enforcement agencies access to 'stored' communications without the need for a telecommunications interception warrant. 'Stored communications' broadly defined includes electronic messages located on a computer, internet server or other equipment, whether read or unread, such as emails, text messages

and voicemail. Under the interim legislation, access to stored communications could be obtained through the use of a search warrant.[1]

In March 2005 the government appointed Anthony Blunn AO (a former Secretary of the Attorney-General's Department) to undertake a review of the regulation of access to communications under the *Telecommunications (Interception) Act 1979*.[2] The review included public submissions and consultations with security and law enforcement agencies, the telecommunications industry, privacy organisations and individuals.

The report titled *the Review of the Regulation of Access to Communications* (known as the Blunn report) was tabled in Parliament on 14 September 2005 and recommended that legislation dealing with access to telecommunications data for security and law enforcement purposes be established.

Upon presenting the Blunn Report to Parliament, the government simultaneously tabled legislation that responded to the first tranche of the report's recommendations. The *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005* included some controversial measures such as 'B Party Intercepts'.[3] See the relevant Bills Digest for a detailed background on that Bill.[4]

This Bill seeks to implement the second tranche of the Blunn recommendations, transferring key security and law enforcements provisions from the *Telecommunications Act 1997* to the TIA Act. The provisions relate to access to telecommunications data, and regulation of telecommunications industry interception obligations. The term 'telecommunications data' refers to information about a communication, as distinct from

---

1. The *Telecommunications (Interception) Amendment (Stored Communications) Act 2004*.

2. Hon. Philip Ruddock MP, Attorney-General, 'Review to ensure telecommunications interception remains relevant in the 21st Century, *Media Release*, 18 March 2005, available at: http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases_2005_First_Quarter_18_March_2005_-_Review_to_ensure_telecommunications_interception_remains_relevant_to_21st_Century_-_0442005, accessed 1 August 2007.

3. The Blunn Report defined B-Party intercepts as 'where there is evidence that a person, other than a person suspected of involvement in the prescribed crime, the B-Party, is using a telecommunications service for communications which are believed to be relevant to the investigation. The B-Party may simply be a conduit for a relevant communication and may not even be aware of the use being made of them.' See: http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Blunnreportofthereviewoftheregulationofaccesstocommunications-August2005, accessed 31 July 2007.

4. Sue Harris-Rimmer, 'Telecommunications (Interception) Amendment Bill 2006', *Bills Digest* no. 102, Parliamentary Library, Canberra, 2005-06.

its content, and includes the sending and receiving parties, and the date, time and duration of the communication.[5]

An Exposure Draft of this Bill was released in February 2007. Industry and interest groups and security agencies were invited to participate in a consultation process, however submissions to the government regarding the exposure draft have not been made public.

The Senate Legal and Constitutional Affairs Committee conducted a Bill Inquiry, presented to the Senate on 1 August 2007. The committee recommended that the Bill be passed, subject to four recommendations regarding

- the definition of 'enforcement agency',
- the determinations of the Communications Access Coordinator,
- oversight by the Inspector-General of Intelligence and Security, and
- independent review of the legislation within five years (the recommendations are detailed further throughout the Digest).[6]

Position of interest groups

A number of groups have made submissions to the Senate inquiry into the Bill. Most submissions have supported the main thrust of the Bill, while pointing out some technical problems with the drafting.[7] Others, such as those from the Australian Privacy Foundation and Electronic Frontiers Australia, argue that the government has misled the community by asserting that there are no major privacy implications in the proposed legislation.[8]

---

5. Hon. Philip Ruddock MP, Attorney-General, 'Second Reading Speech: Telecommunications (Interception and Access) Amendment Bill 2007', *House of Representatives Debates*, 14 June 2007, p. 8.

6. Senate Standing Committee on Legal and Constitutional Affairs, *Report on the Telecommunications (Interception and Access) Amendment Bill 2007*, 1 August 2007, available at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/report/report.pdf, accessed 1 August 2007.

7. As at 30 July 2007, the inquiry had received 27 submissions. See: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sublist.htm.

8. Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional Affairs Committee inquiry into the Telecommunications (Interception and Access) Bill 2007*, July 2007, available at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sub17.pdf, accessed 29 July 2007.

Concerns regarding specific provisions in the Bill are canvassed in the discussion of the Main Provisions.

ALP/Australian Democrat/Greens/Family First policy position

To date there have been no statements from the ALP, Greens or Family First on this Bill. In 2005 the ALP supported the *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005,* while the Australian Democrats and the Greens opposed the Bill.

In a Supplementary Report to the Senate Committee's report on the Bill, the Australian Democrats stated that they believe the Bill as introduced does not adequately account for privacy considerations, and recommended:

- that CrimTrac be removed from the definition of 'enforcement agency'
- that a definition of 'telecommunications data' be included in the Bill
- that prospective telecommunications data, 'in other words location information', be only accessed by enforcement agencies with a warrant
- written authorisations to access mobile telephone location information should be limited to 14 days duration and should not be renewable unless new information suggests that continued interception would likely result in further material information (with renewal up to a maximum of 20 days)
- enforcement agencies consult with a Public Interest Monitor before applying for an interception authorisation (based on a Queensland model), and
- that there be a positive obligation on the part of ASIO or an enforcement agency, where they suspect or have actual knowledge that an employee of a carrier is volunteering personal information, to warn that employee that they are not legally obliged to disclose telecommunications data.[9]

New Explanatory Memorandum

At the public hearing for the Senate Committee inquiry into the Bill, the Attorney-General's Department indicated that it is considering issuing a new Explanatory Memorandum, to clarify some of the examples provided within the document about the

9. 'Supplementary Report with Additional Comments of Dissent by the Australian Democrats', Senate Standing Committee on Legal and Constitutional Affairs, *Report on Telecommunications (Interception and Access) Amendment Bill 2007,* 1 August 2007, p. 37.

intended operation of the legislation.[10] The new Explanatory Memorandum should be available on BillsNet (at http://www.aph.gov.au/bills/) when tabled.

Financial implications

The Explanatory Memorandum states that the Bill will have no financial impact on government.[11] However, for telecommunications carriers, the Bill stipulates that they must meet the costs of developing, installing and maintaining interception and delivery capabilities.[12]

Main provisions

Schedule 1, Part 1 contains the main amendments, proposing to transfer provisions in the Telecommunications Act regarding access to telecommunications data to the TIA Act.

Schedule 1, Part 2 contains consequential amendments to a number of Acts. Schedule 1, Part 3 contains application, saving and transitional provisions.

Key provisions and contentious issues associated with Schedule 1, Part 1 are outlined below.

Schedule 1, Part 1 Definitions

Telecommunications data

While the Bill substantially deals with access to 'telecommunications data', the term is not defined within this Bill or in either the Telecommunications Act or the TIA Act. The Explanatory Memorandum does give a reasonably detailed definition of 'telecommunications data':

> Telecommunications data is information about a telecommunication, but does not include the content or substance of the communication. Telecommunications data is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet based applications including internet browsing and voice over internet telephony.

---

10. Ms Catherine Smith, Attorney-General's Department, *Evidence* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, Transcript of Evidence, 16 July 2007, p. 26.

11. *Explanatory Memorandum*, p. 1.

12. See the Bill: Schedule 1, Chapter 5, Part 5-6 – Allocation of Costs.

> For telephone-based communications, telecommunications data includes subscriber information, the telephone numbers of the parties involved, the time of the call and its duration. In relation to internet based applications, telecommunications data includes the Internet Protocol (IP) address used for the session, the websites visited, and the start and finish time of each session.
>
> Telecommunications data specifically excludes the content or substance of a communication.[13]

This lack of definition for a key term in the Bill is unusual, and was noted in several submissions to the Senate Inquiry. For example, the Law Council of Australia stated:

> The purpose of the Bill is to consolidate and refine the legislative provisions which set out the circumstances in which different types of telecommunications information can be disclosed and accessed for law enforcement purposes.
>
> It is assumed that one of the key aims of the exercise is to ensure that both the privacy rights of individuals and the powers of enforcement agencies are clearly understood. It seems unfortunate, and possibly counterproductive, in those circumstances not to properly define "telecommunications data".[14]

However, the Attorney-General's department has defended the lack of a definition for 'telecommunications data', stating that because of the rapidly changing nature of telecommunications technology, the TIA Act and this Bill have been deliberately left technologically neutral. A department representative told the Senate committee:

> Our concern [is that] defining what technology and call associated data may be now 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.[15]

---

13. *Explanatory Memorandum*, p. 6.

14. Law Council of Australia, *Submission* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, July 2007, p. 14; at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sub20.pdf, accessed 18 July 2007.

15. Ms Catherine Smith, Attorney-General's Department, *Evidence* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, Transcript of Evidence, 16 July 2007, p. 22.

Parliament may wish to consider whether there needs to be some definition of 'telecommunications data' within the Bill. It should be possible to draft a definition which remains technologically neutral but that highlights, as stated by the Attorney-General's representative, that the information being sought is information *about* the communication rather than the communication itself. This is reinforced by proposed s. 172 (stipulating that there is to be no disclosure of the contents or substance of a communication), so it would seem to make sense to also include such a stipulation in the definitions section of the Bill.

However, the Law Council of Australia has gone one step further and requested that a definition be drafted which sets out in positive terms exactly what type of personal information is encompassed within the meaning of 'telecommunications data'.[16]

Enforcement agency

The Bill inserts into the TIA Act a new definition of 'enforcement agency' (**item 6, subsection 5(1)**). The definition is important as an authorised officer of an enforcement agency will be able to authorise the disclosure of historical telecommunications data. The existing TIA Act refers to the Telecommunications Act definition of enforcement agency, which draws together criminal law-enforcement agencies, civil penalty-enforcement agencies, and public revenue agencies such as the Australian Taxation Office. The proposed definition updates the names of some of these agencies, but also allows the government to add new agencies by regulation:

> Subsection 5(1)
>
> ***enforcement agency*** means…
>
> (k) an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purpose of this paragraph.[17]

This addition was criticised by the Law Council of Australia, which argued that the definition of enforcement agency is intended to operate as a safeguard, providing a clear limit on the agencies which have access to an 'extraordinary and invasive' power:

> The Law Council believes that the practice of reserving to the Executive the power to expand definitions of this nature, which are crucial to scope and operation of the *TIA Act*, is of great concern. No reason has been provided for why the efficient operation of the *TIA Act* requires the sort of flexibility afforded the Executive under paragraph (k).[18]

---

16. Law Council of Australia, op. cit, p. 15.

17. Item 6, page 4 of the Bill.

18. Law Council of Australia, op. cit, p. 13.

The proposed definition of enforcement agency also adds the CrimTrac Agency **(5(1)(m))** and any body whose functions include administering a law imposing a pecuniary penalty **(5(1)(n))**.

There has been some criticism of these new additions to the definition of enforcement agency. While the CrimTrac Agency was previously captured in the definition in its former name as the National Exchange of Police Information, it has now been added to the definition as the CrimTrac Agency.

The Attorney-General's Department acknowledged that it is not sure whether CrimTrac should be covered by the TIA regime, stating that they have merely transferred all the agencies covered by the Telecommunications Act over to the TIA Act, and will investigate whether those agencies are actually appropriate for the regime at a 'later date'.[19]

Electronic Frontiers Australia was concerned that the addition of CrimTrac could mean that it would be empowered to obtain stored communications warrants. However, the department argued that as CrimTrac's functions do not include investigations, they would not be able to apply for a stored communications warrant.[20]

The Senate Committee has recommended that CrimTrac be removed from the definition of enforcement agency, stating that

> The inclusion of agencies in this definition provides agencies with intrusive powers so the default position should be that agencies are excluded, unless a positive justification for their inclusion is forthcoming.[21]

---

19. Ms Wendy Kelly, Attorney-General's Department, *Evidence* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, Transcript of Evidence, 16 July 2007, p. 25.

20. Electronic Frontiers Australia Ltd, *Submission* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, July 2007, available at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sub06.pdf, accessed 30 July 2007.

    Attorney-General's Department, *Answers to Questions on Notice*: Senate Legal and Constitutional Affairs Committee, 24 July 2007, p. 22.

21. Senate Standing Committee on Legal and Constitutional Affairs, op. cit, p. 35.

Communications Access Coordinator

Item 11 proposes a new section 6R, creating the new role of Communications Access Coordinator (CAC). It is proposed that the CAC would be the Secretary of the Attorney-General's Department, or a person specified by the Minister, via legislative instrument.

The CAC would replace the role of Agency Coordinator in the Telecommunications Act, with an expanded role as the first point of contact for both the telecommunications industry and agencies in relation to telecommunications information.[22] For example, the CAC is the communication point for carriers and agencies when disagreeing about the location of a delivery point.[23]

Subsection 6R(3) states that unless the context otherwise requires, an act done by or in relation to the CAC is taken to be an act done by or in relation to the CAC on behalf of all the interception agencies.

Chapter 4 – Access to telecommunications data

Item 12 proposes a **new Chapter 4** for the TIA Act: *Access to telecommunications data* and creates a new two-tier access regime, relating to historical data and prospective, or 'near-time' data.

Currently, use and disclosure of telecommunications data is generally prohibited under sections 276-278 of the Telecommunications Act. However, sections 282 and 283 of the Act allow access to telecommunications data for specific law enforcement and national security purposes.

New Chapter 4 would transfer sections 282 and 283 of the Telecommunications Act to the TIA Act. The basis for lawful access to telecommunications data will depend upon whether the authorising body is ASIO (referred to in the Bill as 'The Organisation'), a criminal law-enforcement agency or an enforcement agency.[24]

Proposed Division 2 of Chapter 4 sets out some general provisions, and clearly states that the disclosure of telecommunications content, including a document to the extent that the document contains the contents or substance of a communication, is prohibited.

Proposed Division 3 to the TIA Act outlines the circumstances in which ASIO can access telecommunications data.

---

22. *Explanatory Memorandum*, p. 6.

23. See the Bill: Schedule 1, Chapter 5, Part 5-2, s. 188 (2).

24. *Explanatory Memorandum*, p. 7.

Proposed Division 4 sets out the circumstances in which enforcement agencies can access telecommunications data.

Proposed Division 6 introduces a new offence relating to secondary disclosure.

See below for a more detailed discussion of the above provisions.

Access to data on a prospective basis

Proposed Sections 176 and 180 do not transfer existing provisions of the Telecommunications Act, but create a new scheme for access to prospective information or documents – ie access to telecommunications data in 'near real' time.

Under **176(2)**, ASIO's Director-General, Deputy Director-General, or an SES Band 2 officer (known as eligible persons), would be able to authorise the disclosure of specified information or documents ***that come into existence*** during the period for which the authorisation is in force (emphasis added). The eligible person may also authorise the disclosure of information or documents that existed prior to the time the authorisation came into force (ie historical data). The level of authorisation required for access to prospective data is higher than that required for historical data. Under **175(2)** and **(4)**, the Director-General of ASIO could allow any officer or employee of the organisation to authorise access to historical data, whereas in the case of prospective data, authorisation is limited to SES Band 2 or above.

In making the authorisation, the ASIO officer must be satisfied that the disclosure would be in connection with the performance by ASIO of its functions (**176(4)**).

The authorisation commences at the time the person from whom the disclosure is sought receives notification of the authorisation, and must end within 90 days, unless revoked earlier (**176(5)**).

Similarly, **proposed section 180** allows an authorised officer of a criminal law-enforcement agency to authorise the disclosure of information or documents that come into existence during the period for which the authorisation is in force. In making the authorisation, the officer must be satisfied that the disclosure is reasonably necessary for the investigation of a Commonwealth or State/Territory offence that is punishable by imprisonment for at least three years. The officer must also have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure (**180(5)**).

The authorisation period is half that allowed for ASIO investigations – 45 days (**180(6)**).

These two provisions have attracted significant criticism, particularly because they would seem to allow the use of mobile phone telecommunication data to allow agencies to pin-

point with reasonable accuracy the location of the user – in other words, to use mobile phones as a virtual tracking device in near-real time.

The Law Council of Australia submitted to the Senate inquiry:

> Given the invasion of privacy it represents, the Law Council believes that criminal law-enforcement agencies should require a warrant in order to access prospective telecommunications data and thus use a person's mobile phone as a tracking device.
>
> The Law Council recognises that under Section 39 of the *Surveillance Devices Act 2004*, law enforcement officers are already able to use a tracking device without a warrant in the investigation of a federal offence which carries a maximum penalty of at least 3 years. 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*.[25].

The Inspector-General of Intelligence and Security (IGIS) has requested that ASIO's access to prospective data come under his purview, stating that this would involve periodic visits to ASIO by the IGIS staff, to review all the authorisations granted in the preceding period to ensure there was sufficient justification for their issue and to ensure that requirements set under s. 183 (relating to the form that authorisations must take) are met.[26] The Senate Committee recommended IGIS access in its Bill review.[27]

The Explanatory Memorandum acknowledges that access to prospective telecommunications data has 'increased privacy implications'.[28] Through the Explanatory

---

25. Law Council of Australia, op. cit, p. 7.

26. Inspector-General of Intelligence and Security, *Submission* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, July 2007, available at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sub14.pdf, accessed 25 July 2007.

27. Senate Standing Committee on Legal and Constitutional Affairs, op. cit, p. 35.

28. *Explanatory Memorandum*, p. 12.

Memorandum, the government has argued that these implications are addressed by three more restrictive authorisations that are attached to s. 180:

- disclosure is restricted to an authorised officer of a criminal law-enforcement agency (as opposed to the broader definition of enforcement agency), for the investigation of offences which attract a maximum term of imprisonment of at least three years
- the timeframe for which an authorisation may be in force is limited to 45 days; and
- the authorising officer must have regard to the impact of the authorisation on the privacy of the individual concerned.[29]

The Law Council of Australia questioned the value of the requirement for an authorising officer to 'have regard to' the privacy of the person affected:

> As currently drafted this subsection has little value. It is not clear what it means to "*have regard to*" a person's privacy. How is this intended to impact upon or guide the decision maker in this context?
>
> The Law Council believes that the section should be amended so that it is expressed in terms of a test to be applied by the authorised officer. The Law Council suggests, for example, that the subsection could provide as follows:
>
> "Before making the authorisation, the appropriate authorising officer must be satisfied on reasonable grounds that the likely benefit to the criminal investigation which will result from the disclosure *substantially* outweighs the extent to which the disclosure is likely to interfere with the privacy of any person or persons." [30]

In a similar vein, Privacy NSW suggested proscribing 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.[31]

The Senate Committee took a slightly different approach by recommending that when formulating requirements for documentation of the authorisation and notification process, (**proposed s. 183(2)**), the Communications Access Coordinator should include

---

29. ibid.

30. Law Council of Australia, op. cit, p. 8.

31. Privacy NSW, *Submission* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, July 2007, available at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sub16.pdf, accessed 26 July 2007.

requirements for the consideration and documentation of privacy issues by authorised officers.[32]

At the public hearing for the Senate's inquiry into the Bill, the Attorney-General's department noted that existing section 282 of the Telecommunications Act already allows access to prospective data. As the EM states, advances in technology now mean that prospective data can actually be accessed, including location information via mobile phones and convergent devices. The department's representative told the hearing:

> As to the idea that it can be used for tracking, a mobile phone sends certain signals up to a cell site indicating that we are in a certain location. At the moment the technology is not such that it will pinpoint where either of us are to any level that you could actually track a person to any point.[33]

This viewpoint contradicts that of Electronic Frontiers Australia, who submitted:

> According to commercial mobile phone location-based service suppliers which use location information provided by Australian telecommunications carriers, a mobile phone can currently be located to within 200 metres in metropolitan areas (and within 100 metres in some urban areas). However, new technologies such as Assisted GPS, which is reportedly expected to be introduced in Australia by some carriers in 2007 or 2008, will greatly improve the accuracy of mobile phone location information.[34]

The Attorney-General's department argued against the need for warrants for access to prospective data because the government believes the Bill sets up appropriate safeguards against misuse of the data:

> …we are establishing certain hurdles that [agencies] will have to get through to access this information…we will prescribe all of the hurdles that an agency must go through before they can obtain this information and the kind of form that it has to be in. We will dictate fairly stringent guidelines for how this information is accessed. We obviously do not have any guidelines at the moment, because that it something that will be developed.[35]

---

32. Senate Standing Committee on Legal and Constitutional Affairs, op. cit, p. 35.

33. Ms Catherine Smith, Attorney-General's Department, op. cit, pp. 23–24.

34. Electronic Frontiers Australia Inc, *Submission* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, July 2007, available at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sub06.pdf, accessed 30 July 2007.

35. Ms Catherine Smith, Attorney-General's Department, op. cit, p. 24.

The Internet Industry Association (IIA) has questioned how internet service providers are to provide telecommunications data such as an email's To and From fields, date and probably path/IP address/es, in near real time without breaking the telecommunications interception law which was introduced in last year's Bill dealing with stored communications (stating that an email is considered to be passing over a telecommunications system until it becomes accessible to the intended recipient - effectively until it is in the intended recipient's mail box able to be downloaded. Interception during passage is prohibited).[36]

Secondary disclosure

Division 6 of new Chapter 4 relates to secondary disclosure/use offences. Under **proposed s. 182**, a person commits an offence if information or a document is disclosed to the person as permitted by Division 4, and the person then discloses or uses that document (a penalty of imprisonment for up to two years applies).

Subsections 182(2) and (3) would provide some exemptions, allowing disclosure or use if reasonably necessary for the performance of ASIO of its functions, for the enforcement of criminal law, or for the enforcement of a law imposing a pecuniary penalty, or for the protection of the public revenue. The defendant carries the evidential burden in relation to these subsections.

The Police Federation of Australia has raised its concern regarding **proposed s. 182 (2)(c)**, relating to exemptions if the disclosure or use is reasonably necessary for the enforcement of a law imposing a pecuniary penalty. The Federation is concerned that this may include police disciplinary hearings, as in most states such disciplinary proceedings may attract a pecuniary penalty. The Federation argued that this provision means that police officers would be subject to a lower standard of privacy than the general community. The Federation told the Senate inquiry:

> 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.[37]

---

36. Internet Industry Association, *Submission* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, July 2007, available at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sub26.pdf, accessed 26 July 2007.

37. Mr Mark Burgess, Police Federation of Australia, *Evidence* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, Transcript of Evidence, 16 July 2007, p. 3.

While the Attorney-General wrote to the Police Federation of Australia seeking to assure them that the above scenario was not the intent of the legislation, the Federation has nonetheless requested a re-drafting or clearer definition of the pecuniary penalty provision of **proposed s. 182**.[38]

Authorisation/reporting requirements

Part 4-2 of new Chapter 4 sets out the procedural requirements relating to authorisations. Under **proposed s. 183**, authorisations and notification of authorisations must be in written or electronic (for example, email) form. The Communications Access Coordinator may, with consultation with ACMA and the Privacy Commissioner, set out requirements for the written form of authorisations and notifications (**s. 183 (0 and (3)**).

An internet service provider, Internode Systems Pty Ltd, expressed concern that the wording of Part 4-2 is not clear enough regarding the form of a notification. Internode noted that there is no legislated requirement for a notification to include a copy of the authorisation, or proof that the person giving the notification is in fact authorised to do so, and that the authorisation has been made following due process and that the authorisation does indeed exist.[39]

While Internode's concerns would presumably be able to be allayed by the requirements that the CAC will be able to set for authorisations and notifications (s.183), the company does make a valid point regarding carriers' obligations to ensure that the interceptions they are being asked to undertake are completely legal.

Proposed section 186 requires that each enforcement agency will be required to provide the Minister with an annual report detailing the number of authorisations made under **sections 178-180**, and any other matter requested by the Minister about those authorisations. The reports must be tabled in Parliament, and must not be made in a manner that is likely to enable the identification of a person.

---

38. Police Federation of Australia, *Submission* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, July 2007, available at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sub04.pdf, accessed 30 July 2007.

39. Internode Systems Pty Ltd, *Submission* to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007, July 2007, available at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sub12.pdf, accessed 31 July 2007.

The Law Council of Australia submitted that the reporting requirements should be strengthened so that they are at least as stringent than those set out in the *Surveillance Devices Act 2004*. The Law Council of Australia asked that the section be amended by adding the following requirements:

> (a) the number of applications for authorisation that were refused during that year, and the reasons for refusal; and
>
> (b) the number of arrests made by officers of the agency during that year on the basis (wholly or partly) of telecommunication data obtained under a prospective authorisation issued under s180; and
>
> (c) the number of prosecutions for relevant offences that were commenced during that year in which information obtained as a result of telecommunication data disclosed under a prospective authorisation issued under s180 was given in evidence and the number of those prosecutions in which a person was found guilty.[40]

Chapter 5 – Cooperation with interception agencies

Proposed Chapter 5 to the TIA Act sets out the obligations of telecommunications carriers and service providers to ensure that telecommunications data are capable of being intercepted. This includes:

- the establishment of 'delivery points' from which carriers will transmit intercepted information to ASIO and enforcement agencies (**s. 188**), and details on how disagreements over delivery points are to be determined
- the Minister's ability to make determinations relating to interception capabilities and the obligations of a person covered by a determination (**s. 189-192**)
- the CAC's ability to grant exemptions from interception capability determinations (**s. 192**)
- the requirement for carriers to produce Interception Capability plans which set out how they are going to meet their legal obligation to provide interception capabilities (**Part 5-4**); and
- a stipulation that the costs of developing, installing and maintaining interception and delivery capabilities are to be bourne by the carriers (**Divisions 2 and 3 of Chapter 5**).

The submission to the Senate Inquiry from the Australian Mobile Telecommunications Association (AMTA) generally supported the Bill but raised some concerns regarding determination of delivery points, the redefinition of Interception Capability (regarding what equipment is actually covered by the definition), and development and ACMA's consideration of IC plans. Carriers Vodafone and Telstra also raised some concerns

40. Law Council of Australia, op. cit, p. 9.

regarding costs of implementing IC plans and the lack of consultation before Ministerial or CAC determinations are made.[41]

Schedule 2

Schedule 2 contains further consequential amendments to other Acts, including:

- an amendment to section 5D(3A) of the TIA Act to ensure that all child pornography offences are included in the list of 'serious offences' for which an interception warrant may be sought (**Schedule 2, item 7**), and
- a new **proposed Part 2-4 to the TIA Act**, which would allow the Attorney-General to authorise interception for developing and testing interception capabilities.

Concluding comments

By introducing a two-tier access regime for historical and 'prospective' telecommunications data, the Bill has tightened up the existing regime by limiting access to prospective communications to ASIO and law enforcement agencies, and requiring a higher level of authorisation than that required for historical data.

As the Bill primarily deals with access to 'telecommunications data', it is unusual that the term is not clearly defined. There is an argument that it would be prudent to keep any such definition technologically neutral, given the rapidly evolving pace of the technology. However, given that the Bill proposes intrusive powers, a clear definition of 'telecommunications data' may help to balance privacy concerns against security and enforcement agencies' need to access the information.

Parliament needs to consider whether the higher level of authorisation required for access to prospective telecommunications data adequately meets the privacy concerns that arise, particularly given the development of new technologies and the likelihood that mobile phone 'tracking' is either possible already or will be in the near future. There is some argument for requiring a warrant for access to such information, rather than a written authorisation from within the requesting agency.

There are also some industry concerns regarding implementation of the scheme particularly surrounding delivery points and Interception Capability Plans.

It is also worth noting that the Australian Law Reform Commission (ALRC) is currently reviewing privacy law, including telecommunications interception and privacy law. A

41. See submissions from AMTA, Vodafone and Telstra, at: http://www.aph.gov.au/Senate/committee/legcon_ctte/telecommunications_interception/submissions/sublist.htm.

discussion paper is due for release in September 2007, with the final report due to be given to the Attorney-General six months later, in March 2008.[42] Given this comprehensive review of privacy law the question may arise as to whether this legislation could be delayed to allow consideration and perhaps incorporation of the ALRC's findings on telecommunications privacy issues.

42. Australian Law Reform Commission, *Review of Privacy Act 1988*, at: http://www.alrc.gov.au/inquiries/current/privacy/index.htm, accessed 31 July 2007/

Members, Senators and Parliamentary staff can obtain further information from the Parliamentary Library on (02) 6277 2434.