6

Authority to access stored communications and telecommunications data

Introduction

6.1 This chapter addresses Schedule 2 of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill), which contains amendments in respect of restrictions on access to stored communications and telecommunications data.

6.2 The Committee is mindful that a range of other significant issues concerning the adequacy of the existing regime for access to telecommunications data contained in the *Telecommunications (Interception and Access) Act 1979* (TIA Act) were raised in evidence. Given the interdependent nature of the data retention regime and the telecommunications data access regime the Committee also considers those issues in this chapter.

6.3 In its simplest form, the Bill aims to restrict access to data required to be retained under the regime. It proposes to separate the access to different types of information that is authorised for different types of agencies. Namely the Bill proposes that those agencies considered 'criminal law-enforcement agencies' under the provisions set out in the Bill are authorised to access stored communications under warrant.

6.4 Other agencies, which are considered to be 'enforcement agencies' under the provisions set out in the Bill, are to be authorised to access telecommunications data. Criminal law-enforcement agencies would also be considered to be enforcement agencies, and so would have access to telecommunications data.

6.5 This chapter contains the following sections:

- Access to stored communications under warrant for criminal law enforcement agencies
  - ⇒ Which agencies should be able to access stored communications?
  - ⇒ Authorisation process for accessing stored content
- Access to historical telecommunications data for enforcement agencies
  - ⇒ The basis for a telecommunications data access regime
  - ⇒ Which agencies should be able to access historical telecommunications data?
  - ⇒ Authorisation process for accessing historical telecommunications data
  - ⇒ Destruction of accessed telecommunications data.

Access to stored communications

6.6 The following section examines the proposed access and authorisation processes of agencies which are considered criminal law enforcement agencies under the provisions set out in the Bill.

Which agencies should be able to access stored communications?

The current position

6.7 The TIA Act currently provides that stored communications may be accessed by enforcement agencies under a stored communications warrant to investigate a 'serious contravention' of the law.[1]

6.8 Stored communications are distinct from the telecommunications data being considered in respect of the data retention regime. A stored communication is defined in section 5 of the TIA Act:

> stored communication means a communication that:
>
> (a) is not passing over a telecommunications system; and
>
> (b) is held on equipment that is operated by, and is in the possession of, a carrier; and
>
> (c) cannot be accessed on that equipment, by a person who is not a party to the communications, without the assistance of an employee of the carrier.

1 *Telecommunications (Interception and Access) Act 1979* (Cth), Part 3-3.

6.9 Examples of stored communications include emails or SMS messages held by a carrier.[2] Significantly, access to a stored communication will provide access to the content of the communication.

6.10 'Enforcement agency' is defined in section 5 of the TIA Act as:

> (a) the Australian Federal Police; or
>
> (b) a Police Force of a State; or
>
> (c) the Australian Commission for Law Enforcement Integrity; or
>
> (d) the ACC; or
>
> (e) the Crime Commission; or the Independent Commission Against Corruption; or
>
> (f) the Police Integrity Commission; or
>
> (g) the IBAC; or
>
> (h) the Crime and Misconduct Commission; or
>
> (i) the Corruption and Crime Commission; or
>
> (j) the Independent Commissioner Against Corruption; or
>
> (k) an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purposes of this paragraph; or
>
> (l) a body or organisation responsible to the Ministerial Council for Police and Emergency Management – Police; or
>
> (m) the CrimTrac Agency; or
>
> (n) any body whose functions include:
>
> (i) administering a law imposing a pecuniary penalty; or
>
> (ii) administering a law relating to the protection of the public revenue.

6.11 In its submission the Attorney-General's Department explains that, for the purposes of paragraph (k), the only authority named in the regulations is the Australian Customs and Border Protection Service.[3] It goes on to state:

> Paragraph (n) of the definition of enforcement agency is broad and includes a wide range of Commonwealth, State, Territory and local government agencies. Examples of agencies that have accessed telecommunications data can be found in Chapter 3 of the TIA Act Annual Report 2012-13.[4]

---

2 Attorney-General's Department, *Submission 27*, p. 43.

3 Attorney-General's Department, *Submission 27*, p. 43.

4 Attorney-General's Department, *Submission 27*, p. 44.

6.12 Australian Security Intelligence Organisation (ASIO) interception warrants also authorise access to stored communications.[5]

Proposed amendment to authority to access stored communications

6.13 The Statement of Compatibility with Human Rights in the Bill's Explanatory Memorandum states:

> The Bill will amend the TIA Act to provide that only criminal law-enforcement agencies are able to access stored communications (and to require the preservation of stored communications). Criminal law-enforcement agencies will be defined to mean:
>
> - interception agencies (Commonwealth , State and Territory police and anti-corruption agencies) that are able to obtain warrants to intercept communications under the TIA Act;
> - the Australian Customs and Border Protection Service (Customs);
> - authorities or bodies declared by the Minister as criminal law-enforcement agencies.[6]

6.14 In its submission, the Attorney-General's Department explained the rationale for the proposed amendment:

> Only agencies that have a demonstrated need to access the content of stored communications, and are subject to appropriate privacy and oversight arrangements, should be eligible to do so. In addition, it should be clear either on the face of the TIA Act or in secondary legislation (such as declarations) which agencies are eligible to apply for stored communications warrants or issue preservation notices.
>
> These amendments also recognise the greater privacy sensitivity of stored communications as compared to telecommunications data. Unlike telecommunications data, stored communications reveal the content and the substance of a person's communications with others. The Bill therefore continues the current division in the TIA Act between criminal-law enforcement agencies and enforcement agencies, with the difference being that under the amendments proposed in the Bill only criminal-law enforcement agencies will be able to access stored communications content.[7]

6.15 In respect of the particular agencies listed as criminal law enforcement agencies the Attorney-General's Department noted that:

5 *Telecommunications (Interception and Access) Act 1979* (Cth), section 109.

6 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 [Data Retention Bill], *Explanatory Memorandum*, p. 9.

7 Attorney-General's Department, *Submission 27*, p. 48.

> in practice only the interception agencies, Customs, the Australian Competition and Consumer Commission (ACCC) and ASIC have obtained stored communications warrants in recent years. The reason for the lower number of agencies obtaining stored communications warrants is that an agency must be investigating a serious contravention (which generally excludes offences punishable by less than three years' imprisonment) in order to apply for a stored communications warrant. This high threshold for obtaining a warrant excludes most enforcement agencies from such access in practice.[8]

Attorney-General's discretion in declaring a criminal law enforcement agency

6.16 A number of submitters endorsed the aim of reducing the range of agencies able to access stored communications but did not agree that the Bill satisfactorily achieved this objective. For example, Professor George Williams and Dr Keiran Hardy of the Gilbert + Tobin Centre of Public Law submitted that:

> as the Bill would allow the Attorney-General to declare other authorities and bodies as criminal law enforcement agencies, uncertainty will remain over who will be able to apply for stored communications warrants. In making such a declaration, the Attorney-General must consider a range of factors, including whether the authority is involved in 'investigating serious contraventions'. This wording suggests that only organisations involved in investigating serious breaches of the criminal law will be declared under the provision. However, it is not a limiting factor. The Attorney-General could declare *any* authority or body as a criminal law enforcement agency, so long as he or she considers the specified range of factors in doing so. In particular, the Attorney-General may consider 'any other matter' that he or she considers relevant. It is therefore possible that agencies involved in enforcing fines and protecting the public revenue – including the Australian Taxation Office, local councils, or bodies responsible for enforcing copyright infringements – could be reinstated with the power to apply for warrants to access stored communications.[9]

6.17 In their submission, Professor Williams and Dr Hardy went on to recommend that:

---

8 Attorney-General's Department, *Submission 27*, p. 47.

9 Professor George Williams AO and Dr Keiran Hardy, Gilbert + Tobin Centre of Public Law, University of New South Wales, *Submission 5*, p. 4.

> To achieve greater clarity in the definition of 'criminal law enforcement agency', and to appropriately limit access to stored communications in line with the government's intended purposes, we believe that the matter listed in the proposed s 110(4)(a) should limit the Attorney-General's declaration-making power. That is, the Attorney-General should only be able to declare an authority or body as a criminal law enforcement agency if he or she is satisfied that the agency is involved in 'investigating serious contraventions'.[10]

6.18 The Australian Privacy Foundation made a similar recommendation in relation to the Attorney-General's declaration making power, though recommended the threshold be raised to 'authorities or bodies responsible for investigating serious criminal offences, serious allegations of public corruption, or serious threats to national security'. The Foundation added:

> Moreover, in exercising the determination-making power, the APF recommends that the Attorney-General be specifically required to take into account the effect of a determination on the right to privacy.[11]

6.19 The Australian Communications Consumer Action Network (ACCAN) also held the view that agencies added to the list of criminal law enforcement agencies should 'meet the definition of a body investigating serious offences, as defined in the TIA Act'.[12]

6.20 Other submitters were of the view that the Attorney-General's power to make a declaration avoided the proper Parliamentary scrutiny, and that the power should be removed in its entirety. For example the Internet Society of Australia stated:

> Defining such organisations in regulations instead of the primary legislation means additions to the list will not receive parliamentary scrutiny that should be afforded to the granting of these powers.[13]

6.21 The Internet Society went on to propose the following recommendation:

> Amend the Bill to remove the power of the Attorney-General to expand the Bill's existing list of 'enforcement agencies' and 'criminal law-enforcement agencies'. Alternatively, if recommendations are adopted to limit grounds on which access is given, confine the declaration power of the Attorney-General to

10 Professor Williams and Dr Hardy, *Submission 5*, p. 4.

11 Australian Privacy Foundation, *Submission 75*, p. 24.

12 Australian Communications Consumer Action Network (ACCAN), *Submission 120*, p. 10.

13 Internet Society of Australia, *Submission 122*, p. 6.

> those bodies or agencies that are involved in the prevention and/or detection of a 'serious offence' as defined in the [TIA Act].[14]

6.22 The Law Council of Australia expressed the view that

> the Attorney-General's ability to further expand the agencies which can access stored communications or telecommunications data by way of regulation, unacceptably reduces the level of Parliamentary scrutiny of fundamental elements of the Bill,

and recommended:

> The Bill should be amended so that the agencies that may have access to: …
>
> - Stored communications are by way of a list scheduled to the legislation – not via regulation or other legislative or executive instrument.[15]

6.23 The Senate Standing Committee for the Scrutiny of Bills expressed similar concerns with the declaration power, and added:

> If the proposed approach is to be retained, the committee seeks the Attorney-General's advice as to whether the disallowance process can be amended to provide for increased Parliamentary oversight. This committee notes that this could be achieved by:
>
> - requiring the approval of each House of the Parliament before new regulations come into effect (see, for example, s 10B of the Health Insurance Act 1973); or
> - requiring that regulations be tabled in each House of the Parliament for five sitting days before they come into effect (see, for example, s 79 of the Public Governance, Performance and Accountability Act 2013).[16]

6.24 In response to the proposal for limitation of criminal law enforcement agencies to those in the Bill, the Attorney-General's Department stated in its submission:

> The Attorney-General, as First Law Officer, is well placed to consider whether an authority or body should be an enforcement agency (or a criminal law-enforcement agency) …
>
> The ministerial declaration process is the most appropriate method to determine which of the wide range of agencies across Australia should be able to exercise the non-interception TIA Act powers. This is because ministerial declarations afford flexibility to

14 Internet Society of Australia, *Submission 122*, p. 6.

15 Law Council of Australia, Submission 126, pp. 14-15.

16 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No. 16 of 2014*, p. 6.

> take into account changes made to agency structures and functions. Commonwealth, State and Territory governments regularly change the law enforcement responsibilities of agencies through amendments to administrative arrangements orders and Acts of Parliaments. The speed at which such responsibilities can shift means that the availability of TIA Act powers to a particular body also needs to be both responsive and transparent.[17]

6.25 In response to a question on whether this Committee should be empowered to oversight the Attorney General's declaration making power, Professor George Williams stated:

> It would be a welcome safeguard because it would provide a level of scrutiny that is not otherwise there. Of course, your committee already fulfils similar roles with regard to proscription and other forms of Attorney's decisions. So that would not be inappropriate, but still I think it does not get to the heart of the concern that many people are expressing: that there should be greater clarity about the point of not only which organisations but, as you have indicated, the self-serve nature once declared that they can access the information.[18]

Committee comment

6.26 Given the intrusive nature of warrants that authorise access to stored communications, the Committee considers that the range of agencies able to obtain such warrants needs to be carefully circumscribed to ensure that access to stored communications is limited to agencies with appropriate functions and which are subject to appropriate safeguards.

6.27 The Committee notes the concerns of submitters in respect of the Attorney-General's broad discretion to declare an agency as a criminal law enforcement agency, including agencies which may not have functions in respect of serious contraventions.

6.28 The Committee considers it appropriate for criminal law-enforcement agencies to be listed in the primary legislation. However the Committee accepts that there may be emergency circumstances where a more rapid response is required, and that there is merit in the Attorney-General being able to declare an agency as a criminal law-enforcement agency in such circumstances.

6.29 These declarations should only be made in regard to agencies whose functions include investigating serious contraventions, and such a

17 Attorney-General's Department, *Submission 27*, pp. 48-49.

18 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p.6.

declaration should only be in effect for 40 sittings days of either House of the Parliament. This timeframe enables legislative amendment to be brought before the Parliament and for this Committee to review any proposed amendment to list an agency as a criminal law enforcement agency.

6.30 In regard to the threshold that is to apply for eligibility to be declared a criminal law enforcement agency, the Committee notes the distinction between investigation of a serious offence defined in section 5D of the TIA Act and which applies to interception warrants (broadly, offences punishable by seven years imprisonment or more); and the investigation of a serious contravention, defined in section 5E of the TIA Act, which includes additional offences punishable by 3 years imprisonment or significant fine, and which applies to stored communications warrants. The Committee recognises that there is merit in the view that threshold for agencies which can access telecommunications content under warrant, whether interception or stored communications, should be consistent.

6.31 This Committee previously considered the distinction between the two thresholds in its 2013 report of the *Inquiry into Potential Reforms of Australia's National Security Legislation*. In that inquiry the Committee was not able, upon the evidence before it, to reach a final position about the appropriate threshold for access to telecommunications and stored communication, and recommended the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The Committee reiterates this comment in the context of this inquiry.

6.32 The Committee accepts that, for the purposes of the Bill, the Attorney-General's declaration power should be limited to agencies investigating serious contraventions as defined in section 5E of the TIA Act. The Committee is of the view that the amendments will result in a more appropriate and transparent limitation of agencies than is currently the case. However, the Committee is also of the view that the standardisation of thresholds for agencies to access content of communications should be examined as part of the Government's holistic review of the TIA Act.

6.33 In respect of whether an additional obligation to consider privacy should be included, the Committee notes that the Attorney-General is required under s.110A(4) of the Bill to have regard to whether the declaration would be in the public interest, and also whether the body or authority is required to comply with the Australian Privacy Principles (APPs) or a binding scheme that provides a level of protection of personal information comparable to that provided by the APPs ('a binding scheme'). The Committee also notes Recommendation 8 ii. of the Australian Privacy

Commissioner's submission in which he recommended some additional characteristics which ought to apply to a binding scheme in respect of the declaration of an enforcement agency.[19] The Committee considers those additional characteristics are also appropriate to be applied to consideration of a binding scheme in the context of the Attorney-General's declaration of a criminal law enforcement agency.

Recommendation 17

The Committee recommends that criminal law-enforcement agencies, which are agencies that can obtain a stored communications warrant, be specifically listed in the *Telecommunications (Interception and Access) Act 1979*.

To provide for emergency circumstances, the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare an authority or body as a criminal law-enforcement agency subject to the following conditions:

- **the declaration ceases to have effect after 40 sitting days of either House;**
- **an amendment to specify the authority or body as a criminal law-enforcement agency in legislation should be brought before the Parliament before the expiry of the 40 sitting days; and**
- **the amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sittings days for review and report.**

Further, consistent with the existing provisions of the Bill, the Attorney-General must have regard to the factors listed in proposed paragraphs 110A(4)(b)-(f), and must also be satisfied on reasonable grounds that the functions of the agency include investigating serious contraventions.

19 Office of the Australian Information Commissioner, *Submission 92*, p. 7.

Recommendation 18

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, or its Explanatory Memorandum, or both, be amended to provide that the characteristics of a binding scheme referred to in proposed subparagraph 110A(4)(c)(ii) of the *Telecommunications (Interception and Access) Act 1979* include a mechanism:

- **for monitoring the authority or body's compliance with the scheme; and**
- **to enable individuals to seek recourse if their personal information is mishandled.**

The Committee notes that the Australian Privacy Commissioner currently has these functions in relation to Commonwealth agencies, and some States have privacy commissions which would be well placed to perform these functions within these jurisdictions. Other jurisdictions may need to expand the functions of their existing oversight bodies, or establish new oversight arrangements to meet these requirements.

Recommendation 19

The Committee recommends that the Attorney-General's Department review whether:

- **the agencies which may access the content of communications (either by way of interception warrants or stored communications warrants) under the *Telecommunications (Interception and Access) Act 1979* should be standardised, and**
- **the Attorney-General's declaration power contained in proposed section 110A of the *Telecommunications (Interception and Access) Act 1979* in respect of criminal law-enforcement agencies should be adjusted accordingly.**

The Committee further recommends that the Attorney-General report to Parliament on the findings of the review by the end of the implementation phase of the data retention regime.

Listing of the Australian Securities & Investments Commission as a criminal law enforcement agency

6.34 The proposed definitions of law enforcement agency and criminal law enforcement agency in the Bill do not include the Australian Securities and Investments Commission (ASIC).

6.35 In its submission ASIC stated:

> ASIC, which currently has the ability to access both types of material for certain law enforcement purposes, is excluded from the proposed definition of 'criminal law enforcement agency', even though it has major criminal law enforcement functions and obligations. Accordingly, ASIC's existing powers in this field will be removed if the TIA Bill is enacted in its current form.[20]

6.36 ASIC explained its role as a major criminal law enforcement agency, its current use of stored communications in proving serious offences, and the accountability requirements that apply:

> ASIC is, among other things, a major criminal law enforcement agency. The types of white collar crime investigated and prosecuted by ASIC are both notoriously difficult to prove and capable of causing immense harm to Australia's financial system. This harm includes damage to the integrity of Australia's financial markets, and devastation to individual victims who risk losing their houses and life savings …
>
> ASIC's express criminal law enforcement functions and obligations extend to the investigation and prosecution of "prescribed offences" and "serious offences", as defined in sections 5(1) and 5D of the TIA Act …
>
> Stored communications are a proven valuable source of intelligence to ASIC and constitute crucial evidence for proving serious offences which ASIC is primarily responsible for investigating and prosecuting. Between 1 July 2008 and 30 June 2013 ASIC sought and obtained 19 such warrants …
>
> Any use of telecommunications data or stored communications obtained by ASIC is strictly restricted by:
>
> - obligations imposed on ASIC under the TIA Act;
> - ASIC's obligation to comply with the *Australian Privacy Principles*, which arises because ASIC is an "APP entity" within the meaning of s 6(1) of the *Privacy Act 1988* (Cth) [the Privacy Act]; and

20 Australian Securities and Investments Commission (ASIC), *Submission 24*, p. 2.

- section 127 of the ASIC Act, which imposes an additional obligation upon ASIC to protect the confidentiality of such information.

ASIC also maintains strict internal procedures to protect privacy and ensure we meet all of our obligations when exercising our powers.[21]

6.37 In response to a question from the Committee on this issue, the Attorney-General's Department stated:

> The list of agencies that are included on the face of the legislation are ones that the parliament has already recognised explicitly has those that should have access to data. They are already included either in the Telecommunications (Interception and Access) Act as it currently stands or in regulations made under it as ones who should have access to telecommunications data. The bill reflects the parliament's existing intention that those agencies have access. All other agencies have the ability to seek a declaration, to the extent that they are agencies involved in the enforcement of the criminal law, protection of public revenue et cetera—those categories that I have mentioned—to enable them to access data. You have given one example, ASIC, but there are a number of agencies that do have functions in the enforcement of the criminal law and protection of public revenue and have used data in the past and consider it to be an important part of the tools that they would use.[22]

6.38 In its submission, ASIC argued that making its power contingent on a ministerial declaration introduced legal uncertainty that is not justified:

> It is possible that if ASIC applied to the Minister to be included in such a declaration it would meet the criteria set out in the TIA Bill. However, there is no certainty that the Minister would make a declaration. If a declaration were made, ASIC considers that it would be a sub-optimal outcome because:
>
> - as the making of a declaration would be a challengeable decision, it would result in some legal uncertainty about the nature and extent of ASIC's powers in this field, which would reduce the efficiency of ASIC's investigations and prosecutions and may encourage legal challenges by alleged offenders;
> - such a declaration may be limited by subject matter or be subject to a sunset provision, or be otherwise subject to

21 ASIC, *Submission 24*, pp. 3, 12, 14.

22 Ms Anna Harmer, Acting First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 17 December 2014, p. 23.

restrictive or onerous conditions not applicable to analogous agencies included within the statutory definition; and

- even if a declaration were made by the current Minister at the time the Bill became operational that was not limited by subject matter or time, such a declaration would not bind a future Minister and might be revoked or otherwise varied (the Minister could revoke the declaration at any time under proposed subsection 110A(8)).[23]

6.39 In response to this submission, the Attorney-General's Department stated:

> In terms of the specific issue that ASIC raised this morning, as I understand it, they reflected that perhaps a declaration as an agency would put them on a weaker footing than they might currently be at the moment. With respect to ASIC -- and we have had discussions with them on this point—I do not agree that that is the case. In actual fact, a declaration puts them on a stronger footing than is currently the case. ASIC's ability to access data at the moment relies on their ability to fall within that very broadly and non-specifically cast definition of 'enforcement agency', which does not identify them by name; it relies on them falling within that broad class of agencies who are involved in enforcement of the criminal law and related functions. A declaration as an agency would actually give very specific certainty that ASIC is prescribed for the purposes of accessing data. And I think if anything it puts them on a stronger footing rather making them more susceptible to challenge on the basis on which they can access the data.[24]

6.40 Professor George Williams, in response to a question from the Committee about ASIC's submission, stated:

> I will say that personally I was surprised that ASIC was not on that list given its role in investigating quite serious crimes involving what can be significant criminal penalties. It would be much better for the list to be exhaustive and to include the appropriate bodies in the first place. As to adding bodies in the future: certainly challenges could be possible. The minister makes a decision that could be the subject of a variety of legal challenges, and that ultimately might be quite significant in proceedings because, if you can undermine the ability of the body to get the information, perhaps you might even be able to prevent the admission of that information in court proceedings and so prevent a prosecution.

23 ASIC, *Submission 24*, pp. 16-17.

24 Ms Harmer, *Committee Hansard*, Canberra, 30 January 2015, p. 70.

> That said, I think it is actually going to be quite difficult, if all the procedures are followed, to stop appropriate bodies being declared, and that is because, as I indicated in my opening remarks, the key clause is three, and it actually does not set down any criteria.[25]

6.41 The Uniting Church Justice and International Mission Unit submitted that the definition of criminal law enforcement agency should be expanded to include the Australian Taxation Office (ATO) and ASIC:

> The new law will limit access to the information to be kept to criminal law enforcement agencies … and we believe it should be expanded to include the ATO and ASIC so that these agencies do not suffer a reduction in their capacity to fight tax evasion and corporate fraud respectively.[26]

Committee comment

6.42 The Committee recognises the importance of carefully circumscribing the agencies which are designated as 'criminal law enforcement agencies' to ensure that only agencies involved in investigating serious contraventions of the law and subject to appropriate safeguards may seek warrants to access stored communications.

6.43 On the evidence provided, the Committee considers that ASIC is an appropriate agency to be a 'criminal law enforcement agency'. In particular, the Committee notes that ASIC's functions include investigating serious offences; that access to stored communications is, and will continue to be, of assistance in its investigations of serious offences; and that ASIC is subject to appropriate accountability requirements and safeguards including the Australian Privacy Principles.

6.44 The Committee notes from the Telecommunications (Interception and Access) Act 1979 – Annual Report for the year ending 30 June 2013 that the Australian Competition and Consumer Commission (ACCC) has also previously lawfully accessed stored communications. The Committee has received private correspondence from the ACCC noting the importance of the ability to access telecommunications data and stored communications to the performance of its functions and foreshadowing that, if it is not named in the legislation, it will likely seek a declaration as a criminal law-enforcement agency. The Committee considers that the ACCC is also an appropriate agency to be a 'criminal law-enforcement agency'.

---

25 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 6.

26 Uniting Church in Australia, Justice & International Mission Unit, Synod of Victoria and Tasmania, *Submission 76*, p. 9.

Recommendation 20

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to list the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) as criminal law-enforcement agencies under proposed section 110A of the *Telecommunications (Interception and Access) Act 1979*.

Authorisation process for accessing stored communications

6.45 The Attorney-General's Department explained the current process for accessing stored communications, including the requirement to obtain a stored communications warrant:

> Section 108 of the TIA Act prohibits persons from accessing a stored communication held by a C/CSP, except as provided for in that section (such as access under a warrant).
>
> Section 110 of the TIA Act permits an enforcement agency to apply to an issuing authority (an appointed judicial officer or member of the Administrative Appeals Tribunal) for a stored communications warrant to access stored communications content.
>
> The application can be made in relation to the investigation of a 'serious contravention', which is defined in section 5E of the TIA Act to include (amongst other things) offences punishable by imprisonment by three years or more or contraventions rendering an individual liable to pay a pecuniary penalty of 180 penalty units (currently equivalent to $30,600, on the basis of $170 per penalty unit) or more.
>
> Under section 116 of the TIA Act, an issuing authority may issue a stored communications warrant if the issuing authority is satisfied, amongst other matters, that information likely to be obtained would be likely assist in the investigation of a serious contravention. The issuing authority must also have regard to:
>
> - the impact on any person's privacy;
> - the gravity of the conduct;
> - how much the information would assist in the investigation;
> - whether other methods of investigation would be available or effective.[27]

27 Attorney-General's Department, *Submission 27*, p. 43.

6.46 In its submission, the Australian Privacy Foundation noted that the Bill does not change the threshold for the obtaining of stored communications warrants. The Foundation recommended that the higher 'threshold that applies to real time interceptions – which requires that an investigation should relate to a "serious offence"'[28], should apply to access to stored communications:

> [T}he higher threshold should apply to access to both real-time communications and stored content, and require that such access relate to investigations of serious criminal offences (i.e. offences punishable by imprisonment for at least 7 years, as opposed to the current 3 years applying to stored communications), serious allegations of public corruption, or serious threats to national security. Given the extremely serious privacy implications of access to telecommunications data, the APF further submits that access to such data should be subject to the same thresholds as apply to communications content.[29]

Committee comment

6.47 The Committee notes the distinction between the threshold for an interception warrant being, amongst other things, the investigation of a 'serious offence'; and the threshold for a stored communications warrant being, amongst other things, the investigation of a 'serious contravention'.

6.48 Additionally, the Committee acknowledges the significance of this issue in the context of the current Bill and recognises that there may be some merit in greater consistency in the thresholds for warrants for access to telecommunications content. However, there has been insufficient evidence received to come to a conclusion as to whether, and how, the threshold for a stored communications warrant should be amended.

6.49 Accordingly, the Committee reiterates the recommendation made in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* for an examination of the standardisation of thresholds for accessing the content of communications.[30]

28 Australian Privacy Foundation, *Submission 75*, p. 25.

29 Australian Privacy Foundation, *Submission 75*, p. 25.

30 Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, Recommendation 6, p. 30.

Access to historical telecommunications data

6.50 As indicated earlier, the Bill aims to restrict access to data required to be retained under the regime. It proposes to separate the access to different types of information that is authorised for different types of agencies. The previous section has examined the proposed access and authorisation process for agencies that are considered to be criminal law-enforcement agencies under the provisions set out in the Bill. Criminal law-enforcement agencies are authorised to access stored communications under warrant. Criminal law enforcement agencies are also considered to be enforcement agencies.

6.51 The following section examines the proposed access and authorisations processes for agencies which are considered to be 'enforcement agencies' under the provisions set out in the Bill. The Bill proposes that enforcement agencies be authorised to access historical telecommunications data.

The basis for a telecommunications data access regime

6.52 In recognition of the personal and sensitive nature of the information that telecommunications carriers, carriage service providers and related bodies or persons may hold, the *Telecommunications Act 1997* (Telecommunications Act) protects certain information associated with telecommunications.

6.53 The Telecommunications Act provides that carriers, carriage service providers, and certain other persons must protect the confidentiality of information that relates to:

> (a) the contents of communications that have been, or are being, carried by carriers or carriage service providers; and
>
> (b) carriage services supplied by carriers and carriage service providers; and
>
> (c) the affairs or personal particulars of other persons.[31]

6.54 The penalty for contravening the relevant confidentiality provisions contained in the Telecommunications Act is imprisonment for up to two years.[32]

6.55 The disclosure or use of protected information is authorised in limited circumstances. Chapter 4 of the TIA Act sets out a regime by which certain agencies can authorise the disclosure of such information or documents—with the important exception that it does not permit the disclosure of the

31 *Telecommunications Act 1997*, section 270 (simplified outline).

32 *Telecommunications Act 1997*, Part 13, Division 2.

contents or substance of a communication.[33] In practice this allows the specified agencies to authorise the disclosure of telecommunications data. Significantly, access is not restricted to the categories of telecommunications data proposed to be retained under the Bill.

6.56 The regime in Chapter 4 of the TIA Act distinguishes between access to existing information or documents (referred to as historical telecommunications data) and access to prospective information or documents that will come into existence during the period for which the relevant authorisation is in force (referred to as prospective telecommunications data).

6.57 Law enforcement and security agency evidence consistently highlighted the critical importance of this access regime to their operations. The Australian Federal Police (AFP) stated in its submission:

> Chapter 4 of the TIA Act currently allows a range of agencies to lawfully access telecommunications data by way of authorised request to domestic communications providers. This telecommunications data has provided information fundamental in enabling the AFP to effectively investigate and prevent crime across the full suite of the AFP's functions including counter terrorism, serious and organised crime, firearm and drug trafficking, child protection operations, cybercrime, crimes against humanity such as slavery, people smuggling and human trafficking, as well as community policing in the ACT and airports …
>
> Access to historical telecommunications data is an elementary building block across the vast majority of AFP investigations into serious crimes. Analysis of AFP investigations commenced in the first quarter of 2014-15 confirms that telecommunications data was used in 92% of Counter Terrorism investigations, 100% of Cybercrime investigations, 87% of Child Protection investigations, and 79% of Serious Organised Crime investigations.[34]

6.58 The Police Federation of Australia stated:

> Access to metadata is an essential policing tool. On one hand it is frequently used to eliminate people from ongoing investigations because the data demonstrates that the person concerned was not, at the relevant time, in the relevant place or did not communicate with the suspect. Thus it narrows the field of suspects.

---

33 *Telecommunications (Interception and Access) Act 1979*, section 172.

34 Australian Federal Police (AFP), *Submission 7.1*, pp. 3, 5.

> On the other hand it assists police to establish people involved in a particular incident, relevant connections between individuals involved, the movement of people at particular times, and the incidence of communications between such people.[35]

6.59 South Australia Police stated at a public hearing:

> Access to metadata plays a central role in almost every criminal investigation, including investigations into murder, sexual assault, drug trafficking and kidnapping. In the offence of murder, the ability to actually identify people who have contacted each other is quite critical. It is the same in cases of child exploitation and, obviously, serious and organised crime matters, where you may have people involved in illicit drug-taking or dealing in drugs.[36]

Which agencies should be able to access telecommunications data?

The current position

6.60 The TIA Act currently provides that ASIO or an 'enforcement agency' may authorise the disclosure of historical telecommunications data. The term 'enforcement agency' is defined in section 5 of the TIA Act.[37]

6.61 The Explanatory Memorandum explains the regime in the following terms:

> Access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits an 'enforcement agency' to authorise a carrier to disclose telecommunications data where it is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue … There are separate provisions enabling access by ASIO for purposes relevant to security.
>
> Currently under the TIA Act, an enforcement agency is broadly defined as all agencies empowered to intercept telecommunications content as well as bodies whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue. The range of agencies that are enforcement agencies and which are capable of authorising the disclosure of telecommunications data is broad and includes Commonwealth,

35 Police Federation of Australia, *Submission 72*, p. 2.

36 Mr Paul Dickson, Assistant Commissioner, South Australia Police, *Committee Hansard*, Canberra, 30 January 2015, p. 42.

37 See also paragraphs 6.7 and 6.8 which set out the definition of 'enforcement agency'.

> State, Territory and local government agencies as well as non-government or quasi-government bodies that carry out relevant functions.[38]

6.62 In the *Telecommunications (Interception and Access) Act 1979* – Annual Report for the year ending 30 June 2013, over 70 agencies were identified as having issued authorisations to historic telecommunications data. In its submission the Attorney-General's Department stated:

> The range of agencies that are enforcement agencies and which authorise the disclosure of telecommunications data is broad and includes local councils, State and Commonwealth government departments, agencies such as Centrelink and bodies as the Royal Society for the Prevention of Cruelty to Animals.[39]

Proposed amendment to 'enforcement agency'

6.63 Schedule 2 of the Bill contains an amendment to the definition of enforcement agency.

> Schedule 2 will amend the existing definition of 'enforcement agency' to limit access to telecommunications data to criminal law-enforcement agencies and authorities or bodies that have been declared by the Minister to be an 'enforcement agency'.[40]

6.64 The Explanatory Memorandum notes these amendments are consistent with Recommendation 5 of the previous Committee's *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* that the number of agencies able to access telecommunications data be reduced.[41] That recommendation stated:

> The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.[42]

6.65 In its submission, the Attorney-General's Department explained the effect of the proposed amendment as follows:

---

38 Data Retention Bill, *Explanatory Memorandum*, p. 19.

39 Attorney-General's Department, *Submission 27*, p. 45.

40 Data Retention Bill, *Explanatory Memorandum*, p. 66.

41 Data Retention Bill, *Explanatory Memorandum*, p. 66.

42 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013, p. 46.

> New section 176A will create a new definition of 'enforcement agency' to replace the definition of 'enforcement agency' currently found in section 5 of the TIA Act. The new definition of enforcement agency in section 176A will include criminal law-enforcement agencies (as set out in new section 110A) and any authority or body declared by the Attorney-General to be an enforcement agency …
>
> The new definition of enforcement agency replaces the existing open-ended approach of permitting any agency with functions relating to the enforcement of laws administering a pecuniary penalty or protection of the public revenue from automatically having access to the power to authorise the disclosure of telecommunications and seek stored communication warrants …
>
> Agencies that would no longer be 'enforcement agencies' on the face of the legislation include the Australian Securities and Investments Commission (ASIC), the Australian Taxation Office (ATO), the Department of Defence (in particular, the Australian Defence Force Investigative Service), the Department of Foreign Affairs and Trade (in particular, the Passports Office), the Department of Immigration and Border Protection, Racing NSW, the Victorian Department of Environment and Primary Industries, the Wyndham City Council, and RSPCA South Australia. [43]

6.66 The Department notes that when making a declaration the Attorney-General is required to consider a number of factors:

> When considering whether to declare an authority or body to be an enforcement agency the Attorney-General will be required to consider:
>
> - whether the authority or body has relevant law enforcement functions;
> - whether the obtaining of historic telecommunications data would assist the authority or body in performing those functions;
> - whether the authority or body is governed by an appropriate privacy regime;
> - whether the authority or body will have processes to comply with its obligations under the TIA Act;
> - whether the declaration would be in the public interest.[44]

6.67 In its submission the Department explained the rationale for the amendment:

43 Attorney-General's Department, *Submission 27*, p. 46.

44 Attorney-General's Department, *Submission 27*, p. 46.

> The principle behind the reduction in the number of agencies that can access telecommunications data is that only agencies that have a demonstrated need to access such information, and are subject to appropriate privacy and oversight arrangements, should be permitted to do so. In addition, it should be clear on the face of either the TIA Act or in delegated instruments (such as declarations) which authorities or bodies are enforcement agencies.[45]

6.68 The Department noted that, in principle, all agencies charged to enforce laws should have access to the necessary tools to carry out their functions, but acknowledged the risk of undermining public confidence in the regime if access is too broad or granted to agencies without appropriate controls in place:

> In principle, any agency or organisation charged by an Australian parliament to enforce laws should have access to the necessary tools to carry out their statutory functions. However, the emerging trend of a wider range of smaller, non-traditional agencies and bodies accessing data without external oversight risks undermining public confidence in the integrity of the regime. In particular, these authorities do not always have internal processes, controls and oversight in place to the same degree as traditional law enforcement agencies.[46]

Attorney-General's discretion in declaring an enforcement agency

6.69 A number of submissions expressed support for the Government's aim of reducing the number of agencies able to access telecommunications data. For example the Australian Human Rights Commission stated in its submission:

> The Commission supports the Bill's proposal to confine the number of agencies that may access retained telecommunications data. The Commission notes that this is consistent with the Court of Justice of the European Union's decision, which states that the number of persons authorised to access and subsequently use the communications data should be limited to that which is strictly necessary.[47]

45 Attorney-General's Department, *Submission 27*, p. 45.

46 Attorney-General's Department, *Submission 27*, p. 42.

47 Australian Human Rights Commission, *Submission 42*, p. 10.

6.70 However, a number of submissions also expressed a concern that the change to the definition of enforcement agency does not satisfactorily limit the range of agencies covered by the definition.

6.71 The Law Institute of Victoria stated in its submission:

> Even more concerning is that the Bill leaves wide open the critical question of what authorities or bodies will be listed as an 'enforcement agency' and therefore be able to access the retained data.
>
> This clause gives the Attorney-General the power to list by legislative instrument any authority or body with functions to enforce criminal law or administer a law imposing a pecuniary penalty or relating to the protection of the public revenue. These functions are incredibly broad and reflect the existing and problematic situation where an unknown number of diverse federal, state and even local government entities currently access telecommunications data.
>
> In this context, it seems unlikely that the Bill will significantly limit the range of agencies permitted to access telecommunications data.[48]

6.72 The Institute recommended that 'the agencies which can access telecommunications data must be exhaustively set out in the legislation'.[49]

6.73 Mr Scott Millwood identified a number of risks with the breadth of the declaration regime:

> Further agencies can be added by Regulation at the discretion of the Government, leaving the data retention regime susceptible to scope and purpose creep …
>
> The wider the scope of access, the greater the risk of a breach – 20 agencies with thousands of personnel with access to highly sensitive data on a massive scale, would send a chill through most Chief Security Officers.
>
> A prudent data system would ensure restricted access to the data pool, by limiting both agencies and personnel who have authorised access.[50]

6.74 The Law Council of Australia noted the range of agencies that could potentially be declared, and stated:

---

48 Law Institute of Victoria, *Submission 117*, pp. 11-12.

49 Law Institute of Victoria, *Submission 117*, p. 11.

50 Mr S Millwood, *Submission 121*, pp. 9-10.

> Vesting such a power in the Minister, notwithstanding disallowance procedures available to parliament, may significantly increase the ambit of the legislation and frustrate the intention of the Parliament. Even if a regulation was in force for a short period of time, this would be sufficient for any number of agencies, not previously authorised by the Parliament, to obtain stored communications data or telecommunications data.…
>
> The Bill should be amended so that the agencies that have access to:
>
> … telecommunications data under the scheme are the agencies:
>
> - that may have access to telecommunications data warrants; and
> - listed in a schedule to the legislation – not in regulation or other legislative or executive instrument.[51]

6.75 The Australian Privacy Commissioner expressed a similar view:

> Given public concern about telecommunications data being accessed for the investigation of relatively minor offences, I consider that it is more appropriate that any expansion of the definition of 'enforcement agency' is made by an amendment to the TIA Act itself …[52]

6.76 As noted earlier, in respect to the definition of 'criminal law enforcement agency' the Senate Standing Committee for the Scrutiny of Bills also expressed concerns that the power to include additional enforcement agencies should be in primary legislation rather than by ministerial declaration, and added:

> If the proposed approach is to be retained, the committee seeks the Attorney-General's advice as to whether the disallowance process can be amended to provide for increased Parliamentary oversight. This committee notes that this could be achieved by:
>
> - requiring the approval of each House of the Parliament before new regulations come into effect (see, for example, s 10B of the Health Insurance Act 1973); or
> - requiring that regulations be tabled in each House of the Parliament for five sitting days before they come into effect (see, for example, s 79 of the Public Governance, Performance and Accountability Act 2013).[53]

6.77 The Australian Privacy Commissioner noted the Senate Standing Committee's view, and stated:

---

51 Law Council of Australia, *Submission 126*, p.15.

52 Office of the Australian Information Commissioner, *Submission 92*, p. 22.

53 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No. 16 of 2014*, p. 6.

> As an alternative, the Committee suggested that the disallowance process for this type of ministerial declaration be amended to require the scrutiny of each house of Parliament. Although my preferred approach would be for any amendment to be made by an amendment to the TIA Act, I consider that this could offer an alternative approach.[54]

6.78 The Commissioner further expressed the view that, if the declaration power is to be retained, the Minister, when having regard to the matters set out in subsection 176A(4), should also have regard to:

> whether such a binding scheme provide a mechanism:
> - for monitoring the authority or body's compliance with the scheme, and
> - to enable individuals to seek recourse if their personal information is mishandled.[55]

6.79 In addition, the Commissioner recommended that subsection 176A(5) of the Bill be amended to require the Commissioner to be consulted before making a declaration under subsection 176A(3).[56]

6.80 In response to concerns about the declaration process, the Attorney-General's Department stated in its submission:

> The Attorney-General, as First Law Officer, is well placed to consider whether an authority or body should be an enforcement agency (or a criminal law-enforcement agency) …
>
> The ministerial declaration process is the most appropriate method to determine which of the wide range of agencies across Australia should be able to exercise the non-interception TIA Act powers. This is because ministerial declarations afford flexibility to take into account changes made to agency structures and functions. Commonwealth, State and Territory governments regularly change the law enforcement responsibilities of agencies through amendments to administrative arrangements orders and Acts of Parliaments. The speed at which such responsibilities can shift means that the availability of TIA Act powers to a particular body also needs to be both responsive and transparent.[57]

6.81 The Department also noted that the Attorney-General will have the ability to revoke a declaration and will have the ability to impose conditions, providing 'a further ability to restrict access to telecommunications data in

54 Office of the Australian Information Commissioner, *Submission 92*, p. 23.
55 Office of the Australian Information Commissioner, *Submission 92*, p. 23.
56 Office of the Australian Information Commissioner, *Submission 92*, p. 24.
57 Attorney-General's Department, *Submission 27*, pp. 48-49.

a manner consistent with and proportionate to the functions of the agency'.[58]

6.82 Professor George Williams and Dr Keiran Hardy of the Gilbert + Tobin Centre of Public Law proposed that enforcement agencies should be defined with greater specificity, but identified an alternative in the event that it is not practicable to list all relevant agencies in the legislation:

> If it is not practicable to list all relevant authorities that will have access to metadata, the legislation should at least specify the types of authorities that will have access (such as local council, and authorities responsible for taxation). These categories should be appropriately considered by Parliament as part of the primary legislation. In addition, the power to declare authorities or bodies as enforcement agencies should be limited to those organisations that enforce the criminal law, impose pecuniary penalties or protect the public revenue.[59]

6.83 A number of submitters identified similar concerns with the potential breadth of the range of enforcement agencies, and proposed instead that the Attorney-General's declaration making power should be limited to agencies investigating serious offences or threats to national security. For example, Open Knowledge Australia stated that:

> the range of agencies that could gain access to telecommunications data if the Bill is passed in its current form is, in fact, broader then under the present regime.
>
> Given the extent and sensitive nature of the data likely to be retained, OKFNau urges that the range of enforcement agencies given access to telecommunications data retained under the Bill be limited to those investigating serious criminal offences and activities threatening national security.[60]

6.84 The councils for civil liberties across Australia also expressed their concerns with the breadth of the declaration power, and that some additional clear criteria should be added to the declaration power:

> The issue of who will have access to stored telecommunications data of every internet provider customer in Australia is of great significance in the determination of the proportionality of this intrusion into the privacy rights of persons who are not suspected of any involvement in unlawful activity …

---

58 Attorney-General's Department, *Submission 27*, p. 48.

59 Professor Williams and Dr Hardy, *Submission 5*, p. 5.

60 Open Knowledge Australia, *Submission 110*, p. 4.

> The CCLS recommend that a clearer and tighter definition of types of organisation which can be declared as enforcement agencies be specified in the bill and these be limited to those whose functions include:
>
> - i) enforcement of the criminal law; or administering a law imposing a pecuniary penalty; or administering a law relating to the protection of the public revenue; and
> - ii) some additional clear criteria which would ensure that only agencies dealing with serious crime or serious unlawful actions are included.[61]

6.85 The Australian Privacy Foundation was of the view that a declaration power should be limited to those agencies able to access content:

> [A]ccess to telecommunications data (or metadata) now poses equivalent risks to privacy, and in some instances manifestly greater risks, than access to communications content. Consequently, the APF recommends that there should be no distinction between authorities and bodies entitled to apply for a stored communications warrant and those entitled to access telecommunications data, such that the ability to access such data should be confined to authorities or bodies responsible for investigating serious criminal offences, serious allegations of public corruption, or serious threats to national security.[62]

6.86 In response to a query as to whether any thought had been given to a practical way to put some 'hard markers' in the declaration power to exclude some groups and some functions that are clearly outside the scope of what is intended, the Attorney-General's Department stated:

> The bill, I think, in some respects is intended to do precisely that. It identifies the class of agencies that may have a legitimate need to access data in the performance of their functions. So agencies that are involved in the enforcement of the criminal law, the administration of pecuniary penalties and the protection of public revenue are ones that the parliament has already envisaged through the legislation as it currently stands may be have a need to access data. The bill imposes an additional limitation upon that and says that, rather than your membership of that broad class creating an ability to access data, in addition there should be a requirement that the Attorney-General explicitly consider the extent to which data is required in support of those particular functions, the particular oversight arrangements that apply for an

61 Councils for civil liberties across Australia, *Submission 129*, p. 20.

62 Australian Privacy Foundation, *Submission 75*, p. 24.

> agency that wishes to access data and the extent to which that agency is the subject of binding privacy obligations. So the bill does insert a new mechanism to ensure that it is very clear which agencies are included and to provide key thresholds around that. There will be a clear list of agencies that have access to data, and for those that are not in there it will be clear that they do not.[63]

6.87 When asked by the Committee if there was a situation where a non-government organisation, body, or group, could ever be declared, the Department stated:

> The threshold around who can be declared is one that is defined by reference to the function—so, as I have said, enforcement of the criminal law and/or laws protecting public revenue or imposing a pecuniary penalty. It is typically the case that governments confer those functions upon government agencies however they might be described. We have seen over the operation of the current arrangements that a number of bodies have functions in that regard and, therefore, have had access to the data arrangements. So the precise constitution of a body that would be the subject of a declaration is naturally determined by the extent to which governments confer upon agencies or bodies functions in relation to the enforcement of criminal law. Enforcement of the criminal law is typically regarded as a function of the state, and so, as a general observation, I would say that those functions are conferred on government bodies, but the precise definition that is used in the legislation is around the characterisation of functions of those bodies.[64]

Committee comment

6.88 The Committee welcomes the Attorney-General's reform of the scope of agencies which may access telecommunications data. This measure implements the previous Committee's Recommendation 5 in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*.

6.89 The Committee recognises that the degree of intrusion into privacy resulting from access to telecommunications data will depend significantly on the type and amount of telecommunications data accessed. The Committee considers that in the context of the modern telecommunications environment, and in particular the proposed data

63 Ms Harmer, *Committee Hansard*, Canberra, 17 December 2014, p. 23.

64 Ms Harmer, *Committee Hansard*, Canberra, 17 December 2014, p. 29.

retention regime, there is potential for access to telecommunications data to amount to a very significant intrusion into privacy by an agency.

6.90 The Committee notes the concerns of submitters in respect of the Attorney-General's broad discretion to declare an agency as an 'enforcement agency', including agencies which may not have functions in respect of serious contraventions of the law. In particular, while the Attorney-General is required to have regard to certain matters, his or her discretion to declare an agency an enforcement agency is not otherwise fettered on the face of the legislation.

6.91 For this reason, consistent with proposed measures to safeguard access to stored communications, the Committee considers that those agencies able to access telecommunications data should be listed in the legislation.

6.92 The Committee notes that excluded agencies may be able to access telecommunications data as part of a joint investigation with a listed enforcement agency.[65]

6.93 However the Committee also accepts that there may be emergency circumstances where a more rapid response is required, and that there is merit in the Attorney-General being able to declare an agency as an enforcement agency. In these circumstances, the Committee considers it appropriate to direct the Attorney-General's declaration power to those agencies whose functions include enforcement of the criminal law, administering a law imposing a pecuniary penalty, or administering a law relating to the protection of the public revenue.

6.94 Further, such a declaration should only be in effect for 40 sittings day of either House of the Parliament. This timeframe enables legislative amendment to be brought before the Parliament and for this Committee to review any proposed amendment to list an agency as an enforcement agency.

6.95 While the Committee considers it would be a matter of good practice for the Attorney-General to consult with the Australian Privacy Commissioner and Ombudsman before making a declaration, it is not considered necessary to insert a mandatory consultation requirement for this in the legislation.

6.96 When considering whether an authority or body is required to comply with a binding scheme that provides a level of protection of personal information that is comparable to the level provided by the Australian Privacy Principles, for the purposes of proposed subparagraph 176A(4)(c)(ii), the Committee agrees with the Australian Privacy Commissioner's proposal that regard should also be had to whether such

65 Attorney-General's Department, *Submission 27*, p. 45.

a binding scheme provides mechanisms for monitoring an agency's compliance with the scheme, and enabling individuals to see recourse if personal information is mishandled.

Recommendation 21

The Committee recommends that enforcement agencies, which are agencies authorised to access telecommunications data under internal authorisation, be specifically listed in the *Telecommunications (Interception and Access) Act 1979*.

To provide for emergency circumstances the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare an authority or body as an enforcement agency subject to the following conditions:

- **the declaration ceases to have effect after 40 sitting days of either House;**
- **an amendment to specify the authority or body as an enforcement agency in legislation should be brought before the Parliament before the expiry of the 40 sitting days; and**
- **the amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sitting days for review and report.**

Further, consistent with the existing provisions of the Bill, the Attorney-General must have regard to the factors listed in proposed paragraphs 176A(4)(b)-(f), and must also be satisfied on reasonable grounds that the functions of the agency include enforcement of the criminal law, administering a law imposing a pecuniary penalty, or administering a law relating to the protection of the public revenue.

Recommendation 22

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, or the Explanatory Memorandum, or both, be amended to provide that the characteristics of a binding scheme referred to in proposed subparagraph 176A(4)(c)(ii) of the *Telecommunications (Interception and Access) Act 1979* include a mechanism:

- **for monitoring the authority or body's compliance with the scheme; and**
- **to enable individuals to seek recourse if their personal information is mishandled.**

The Committee notes that the Australian Privacy Commissioner currently has these functions in relation to Commonwealth agencies, and some States have privacy commissions which would be well placed to perform these functions within these jurisdictions. Other jurisdictions may need to expand the functions of their existing oversight bodies, or establish new oversight arrangements to meet these requirements.

Access for civil litigation purposes

6.97 Currently, access to telecommunications data is not restricted solely to ASIO and enforcement agencies. Telecommunications data may be lawfully disclosed by telecommunications carriers and carriage service providers to other bodies and persons in specific circumstances as set out in Division 3 of Part 13 of the Telecommunications Act. That Division, amongst other things, makes provision for disclosure where required or authorised by or under law, and by witnesses summoned to give evidence or produce documents.[66]

6.98 A number of submitters expressed concerns, in the context of the data retention scheme, that telecommunications data will be able to be accessed for civil litigation or other purposes not related to law enforcement. For example, the Communications Alliance and Australian Mobile Telecommunications Association (AMTA) raised concerns in respect of the implications of the availability of retained metadata for use in civil proceedings:

> There has been understandable public concern expressed that, once it is clear that increased volumes of metadata are being

66 *Telecommunications Act 1997* (Cth), s.280.

> retained by CSPs for a specified period, these data will become a 'honey-pot' for civil litigants, who may seek court orders to obtain access to metadata for use in civil proceedings. Such actions could stem from Family Law cases and all manner of commercial disputes.
>
> If such a practice were to become commonplace there are serious financial implications to CSPs. Moreover, such a practice would be manifestly outside the intended objectives of a data retention regime, and therefore should be guarded against.[67]

6.99 Communications Alliance elaborated further at a public hearing:

> At the outset, we recognise this may be a difficult issue to tackle, given that civil litigants do have rights to seek discovery for those sorts of data. I guess our concern is that, once it is known—through the requirements of the data set—exactly what data is being retained by each service provider and for how long, that may generate a tsunami of action in commercial disputes, in marital disputes and in many other cases where the data is being mined in circumstances where we may not be able to recover costs for all sorts of purposes that the data retention bill was not designed to facilitate …
>
> Our concern, I guess, is that this is a high-profile exercise and it will put it very clearly in the public consciousness that a defined set of data is available from every service provider, and we think it may start an industry, if you like …[68]

6.100 Mr Alexander Lynch expressed the view that access to telecommunications data without warrant should be limited to national security and serious criminal investigations, and should not be available for civil litigation:

> Metadata should be available without a warrant only for national security investigations and the investigation of serious crimes. Data retention legislation should specify that the metadata being retained is only available to named intelligence, police, border and biosecurity agencies only for those specific purposes, and that it is not legal nor is it the Government's intent that the records be available for other purposes, such as civil litigation.[69]

---

67 Communications Alliance Ltd and Australian Mobile Telecommunications Association (AMTA), *Submission 6*, pp. 14-15.

68 Mr John Stanton, CEO, Communications Alliance, *Committee Hansard*, Canberra, 17 December 2015, p. , Canberra, 17 December 2015, p. 5.

69 Mr Alexander Lynch, *Submission 1*, p. 1.

6.101 Mr Chris Berg of the Institute of Public Affairs also expressed concerns with the availability of telecommunications data for civil proceedings :

> It is also deeply concerning that mandatory data retention will inevitably be a feature of civil litigation. Any information that is created can be accessed by a subpoena with the permission of a court. While many citizens may believe that democratic governments act in their own best interest most of the time, they might not believe the same about their fellow citizens, who they may have to face in future litigation. This has been the experience of other nations with data retention laws. One investigation of Polish data retention laws found that 'more and more often traffic and location data is requested by the parties in civil disputes such as divorce and alimentary disputes.' The prospect of a semi-permanent record of travel data being available for personal litigation is unlikely to be welcomed by Australian voters.[70]

6.102 Mr Iain Muir foreshadowed access of telecommunications data by copyright holders for the purposes of pursuing those in breach of their rights:

> Copyright holders will demand access to these stores of metadata likely pressing down on service providers via threats of litigation. These will be used in turn to self police their intellectual property. Typically done via threats of legal action with pressure to settle out of court for whatever they see fit, mostly from those who can least afford it. Furthermore the victims of such unfair litigation may not have even downloaded the offending file as theft of wi-fi is depressingly common.[71]

6.103 The Australian Privacy Foundation also noted a risk of scope creep in use of the data in both civil and criminal litigation:

> Given the volume of data that will be retained by carriers and ISPs, there will be considerable pressure for such data to be accessed and used for purposes other than law enforcement and national security. In particular, there will be immense pressure for the data to be accessed and used in both civil and criminal legal proceedings by parties who are not authorised to access the data under the TIA Act. In terms of criminal law proceedings, prosecutors will have clear incentives to seek to access data on the basis of speculation alone; while defence lawyers will have incentives to request access to potentially exculpate their clients.

---

70 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. [6].

71 Mr Iain Muir, *Submission 28*, p. 1.

> And further, Courts may clearly order the disclosure of records wherever relevant across a broad range of cases. In terms of civil litigation, the data exists as a 'honey-pot' for a broad range of actors. Parties to disputes in family law, and in all manner of commercial disputes (involving, for example, trade secrets, intellectual property, and defamation) will likely seek disclosure of retained metadata. For instance, Communications Minister Turnbull and the AFP have announced that data records could be made available for copyright litigation purposes. Claims that the data will not be used by agencies for purposes other than those permitted under the TIA Act are simply disingenuous, as the Bill does not impose any limitations on access to the data by means of other legal avenues, including conventional litigation processes.[72]

6.104 The Law Institute of Victoria, in its supplementary submission, proposed that access should be prohibited otherwise than in accordance with the provisions of the TIA Act:

> The LIV strongly recommends access to telecommunications data should be limited to the purposes of the Bill, i.e. preventing, detecting and prosecuting crime and terrorist activities. As such, access should be prohibited otherwise than in accordance with the provisions of the TIA Act. Such a prohibition should apply to the courts, as well as other persons. Such a provision could be modelled on s 57 of the *Meat Industry Act 1993 (Vic)*.
>
> To ensure that telecommunications providers can still use the data to deliver services, there should also be an exception to the prohibition, which permits telecommunications providers to use and disclose the telecommunications data for business purposes necessary to deliver the telecommunications or internet services.[73]

6.105 Mr Scott Millwood included a similar recommendation in his submission:

> An appropriate amendment would prohibit Service Providers from providing metadata about communications to any third party, except as required to provide their services or as mandated by the Telecommunications (Interception and Access) Act or permitted under the Privacy Act.
>
> This would limit scope and ensure that the concern that metadata might be accessed for other legal processes, including civil litigation, is addressed.

---

72 Australian Privacy Foundation, *Submission 75*, pp. 15–16.

73 Law Institute of Victoria, *Submission 117.1*, p. [9].

> It is also recommended in the interests of transparency, accountability and good governance.[74]

6.106 Telstra noted that it expected to receive an increase in court orders to make customer data available, and recommended that industry be given the ability to recover costs:

> If enacted, the Data Retention Bill would increase the volume of data we are required to retain and is likely to also raise public awareness of this fact. As a result, we expect to receive an increase in the number of court orders we receive to make customer data available to the courts as part of civil litigation proceedings that otherwise does not involve Telstra. These court orders can already be quite resource intensive to comply with today as they often require telecommunications company to interpret data for the courts. Also industry does not have the option of cost recovery on court orders. Telstra recommends that industry be given the ability to recover the costs arising in providing information in response to court orders.[75]

6.107 In its submission Telstra also noted a risk of agencies excluded from the TIA Act regime using other statutory powers to access telecommunications data:

> However, we note that as a result of the proposed amendments to the Telecommunications (Interception and Access) Act 1979, there is now uncertainty as to whether these organisations can revert to using coercive notice to produce or investigatory powers (provided to these bodies under other State or Commonwealth legislation) to access this data. We would recommend additional wording be included in the legislation to ensure there is no back door for these organisations to get access to retained data under other pieces of legislation.[76]

6.108 The Law Council of Australia noted the ability for agencies and other persons to obtain access to telecommunications data under other laws and recommended that access to telecommunications data under other laws or by court process should be precluded:

> The Bill does not limit in any way disclosures of data required to be retained where those disclosures are mandated by laws other than the Bill …

---

74 Mr Scott Millwood, *Submission 121*, p. 15.

75 Telstra, *Submission 112*, p. 5.

76 Telstra, *Submission 112*, p. 4.

> A variety of Federal, State and Territory Acts empower particular agencies to compel disclosure. For example, section 29 of the *Crime Commission Act 2012* (NSW) provides that an executive officer with special legal qualifications may, by notice in writing served on a person require the person to appear before the Commission at a particular time and place and produce to that officer a document or thing specified in the notice, being a document or thing that is relevant to an investigation.
>
> Subpoenas are frequently already issued to third parties by courts, including ISPs, to produce records. Further, parties to prospective or current litigation might seek such retained data as part of the discovery.
>
> In the absence of any restriction upon access to telecommunications data under other Federal, State or Territory laws or court process requiring disclosure of information or documents, there are obvious concerns about the privacy and security of telecommunications data held by authorised collecting agencies. Significant risks include attempting to determine journalists' sources, cases involving alleged infringement of online copyright, family law proceedings, civil claims involving use of machinery or motor vehicles, class actions or other legal proceedings.
>
> The Law Council recommends that access authorised by other Federal, State, or Territory laws, or pursuant to court process should be precluded to ensure that the impact of the Bill is clear and limited to achieving its stated purpose.[77]

6.109 The Law Council of Australia, also noted alternatives in a public hearing:

> Our submission is that the bill should be amended to preclude access. An alternative submission would be that it proscribes access so that access would only be permitted if and where particular access or classes of access were permitted by regulation …
>
> I can envisage that regulations might allow access either by agency, by specified level of court or by class of action.[78]

6.110 In response to a question from this Committee as to whether there may need to be some change in respect of this issue, the Attorney-General's Department stated:

---

77 Law Council of Australia, *Submission 126*, p. 21.

78 Mr Peter Leonard, Chairperson, Media and Communications Committee, Business Law Section, Law Council of Australia, *Committee Hansard*, Canberra, 30 January 2015, p. 37.

> It is the case, obviously, that data that is already available and data that will become available in accordance with data retention is available and amenable to other lawful process, including in the civil space whether that be through subpoena or other orders for production. Production in other contexts itself raises a number of challenges and the ability for persons in those proceedings to adduce such evidence as is relevant to their proceedings, and of course it extends into such matters as family law, other commercial situations other than the rights space, which has been the subject of some coverage. It is the case that that data would be available and it has been for some time and is amenable to that process.[79]

6.111 In a supplementary submission the Attorney-General's Department expressed concerns with restricting the availability of telecommunications data so as to prevent its availability for civil litigation:

> Access to telecommunications in civil and administrative proceedings is, and will continue to be important for plaintiffs to protect their interests and rights. Data can be of particular importance where civil proceedings are closely linked to a criminal matter. Proceedings where data may be relevant include proceeds of crime actions, civil child protection investigations, apprehended violence orders and actions involving incidents of stalking and harassment, which often involve the use of a carriage service. In the Department's view, there is a strong public interest in telecommunications data continuing to be accessible to plaintiffs.
>
> … Limiting or restricting access to telecommunications data in court proceedings may also give rise to constitutional risks relating to the separation of powers by limiting the scope of judicial discretion to obtain the information necessary to assist the court in exercising its judicial function.[80]

Committee comment

6.112 The Committee notes that telecommunications data is currently accessed under existing laws by persons or entities other than law enforcement and national security agencies using exceptions to the prohibition on disclosure contained in Division 3 of Part 13 of the Telecommunications Act. The Committee considers that the majority of these exceptions, for example in respect of emergency management, or the business needs of service providers, should continue to apply.

79 Ms Harmer, *Committee Hansard*, Canberra, 17 December 2014, p. 22.

80 Attorney-General's Department, *Submission 27.3*, p. 1.

6.113 However, the Committee holds concerns in respect of a possible increase in the frequency and volume of telecommunications data accessed by civil litigants as a result of the implementation of the proposed data retention regime, and has paid careful heed to suggestions that such access be restricted.

6.114 The Committee is aware of the potential for unintended consequences resulting from a prohibition on courts authorising access to data retained under the data retention scheme. The potential for possible interference with judicial power was also raised in evidence.

6.115 Nonetheless, the Committee considers that the proposed data retention regime is being established specifically for law enforcement and national security purposes and that as a general principle it would be inappropriate for the data retained under that regime to be drawn upon as a new source of evidence in civil disputes.

6.116 The Committee considers that the Bill should be amended to include a prohibition on civil litigant access to telecommunications data retained for the purpose of complying with the mandatory data retention regime. The Committee considers that this prohibition should only apply in respect of data retained solely for the purposes of the data retention regime. It should not apply more broadly to telecommunications data retained for other purposes, such as data that is currently retained for the business needs of the service provider.

6.117 The Committee considers that the amendment should include a regulation making power to enable provision for appropriate exclusions, such as family law proceedings relating to violence or international child abduction cases, and that the Minister for Communications and Attorney-General review this measure.

6.118 The Committee does not wish to prescribe how a regulatory power would work when it comes to what should be excluded. This will be a matter that will have to be reviewed and further considered by the Attorney-General.

Recommendation 23

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to prohibit civil litigants from being able to access telecommunications data that is held by a service provider solely for the purpose of complying with the mandatory data retention regime.

To enable appropriate exceptions to this prohibition the Committee recommends that a regulation making power be included.

Further, the Committee recommends that the Minister for Communications and the Attorney-General review this measure and report to the Parliament on the findings of that review by the end of the implementation phase of the Bill.

Personal access

6.119 In its submission, the Law Council of Australia highlighted the importance of individuals being able to seek access to their own telecommunications data:

> An exception should be provided for individuals seeking to access their own telecommunications data. This may be essential, for example, in a criminal trial where an individual believes that telecommunications data may establish their innocence. If government agencies are able to access the telecommunications data of individuals to establish a prosecution, the Law Council considers that it is also appropriate for individual's to access such data to be able to establish a defence, or to understand the evidence and charges against them.[81]

6.120 The Pirate Party Australia expressed that there was some uncertainty as to whether users would be able to access telecommunications data they have generated.

> It is unclear whether provision will be made for subscribers and users to inspect or otherwise gain access to the retained data they and people using their accounts have generated. Under the Privacy Act 1988 companies have a general obligation to allow individuals to inspect and correct personal data that they hold. However, journalist Ben Grubb was (and appears to remain) engaged in a dispute with Telstra over a request for their personal telecommunications data. This issue ought to be resolved, and

81 Law Council of Australia, *Submission 126*, p. 21.

> preferably individuals would be permitted to inspect the records held.[82]

6.121 Telecommunications industry representatives raised concerns in their submissions in respect of the costs of personal access by customers to telecommunications data stored as part of the data retention regime.

6.122 The Communications Alliance and AMTA proposed that it should be explicit that carriers and carriage service providers are not required to provide individuals access on demand to all retained data, while reinforcing their right to access to their stored personal information:

> The Bill does not explicitly address the question of whether individuals should have the right under Australian Privacy Principle 12, to make demands upon CSPs to provide access to their personal metadata, especially the metadata captured by the mandatory data retention scheme …
>
> The size and cost of the task for a CSP to pull together and make available all the metadata relating to an individual should not be underestimated. The prospect of potentially millions of Australians making such requests to CSPs is little short of frightening. Such a scenario would generate enormous expense and resource demands on CSPs, for no clear or positive outcome. CSPs would need to create purpose-built security and management systems to meet the additional demands imposed on them by this new requirement.
>
> The Associations stress that we are not advocating any restriction on customer access to the Personal Information stored by CSPs about their customers – data such as billing information, address and identification details. This information should continue to be freely available to customers …[83]

6.123 When asked at a public hearing for comment on this concern, the Attorney-General's Department stated:

> There are a couple of things we can provide some preliminary comments on, at this stage. As Communications Alliance has probably flagged, there are arrangements under which people can access their own personal information. The Privacy Act provides a mechanism for individuals to request their own personal information. What is 'personal information' depends on the circumstances, but it is information that reasonably leads to the identification of a particular individual. What that is will depend

82 Pirate Party Australia, *Submission 124*, p. 12.

83 Communications Alliance and AMTA, *Submission 6*, p. [15].

> on the circumstances and will depend on what the information is, the circumstances in which it is received and how access is arranged. Particularly in the telecommunications context, that can vary according to network configurations—whether a particular data point is one that identifies an individual. Nevertheless, it is the case that, to the extent that carriers have personal information, individuals may apply to those carriers and request their personal information. Indeed, industry is entitled to recover the reasonable cost and is entitled to charge for the provision of personal information under that Privacy Act framework.[84]

6.124 In his submission, the Australian Privacy Commissioner provided a detailed response to the concerns expressed by the Communications Alliance and AMTA:

> Organisations within the meaning of the Privacy Act are required to comply with the APPs when handling personal information that they collect and retain. If the Bill is passed, this will include personal information collected and retained in compliance with the proposed data retention scheme by service providers covered by the Privacy Act. APP 12 requires those service providers to give an individual access to any personal information that the provider holds about the individual on request, subject to certain exceptions (such as where giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body). APP 12 also sets out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.
>
> Under APP 12, an organisation may impose a charge on an individual for giving access to their personal information, provided the charge is not excessive …[85]

6.125 In its submission, Telstra identified the potential for an increased regulatory burden imposed by the Privacy Act in respect of retained data:

> If compliance with the Bill increases the amount of personally identifiable information we hold about our customers, then it will increase the regulatory burden imposed on industry by the Privacy Act …

---

84 Ms Harmer, *Committee Hansard*, Canberra, 17 December 2014, p. 30.

85 Office of the Australian Information Commissioner, *Submission 92*, pp 36-37.

> On top of our obligation under the Privacy Act to protect against data breaches, the manner in which the data will need to be held to comply with the Bill may mean that Telstra could be required to make this data available to individual customers in response to an access request for personal information.[86]

6.126 Telstra noted in such a case that additional costs will be incurred, and that such costs may not be able to be fully recovered by charging customers for providing access to personal information:

> Providing this information to customers is not the same as providing information to authorised enforcement agencies and would involve additional costs, for example in verifying a customer's identity and redacting information on incoming calls to protect the privacy of other individuals. There is a fundamental difference between responding to a reasonably precise and limited request from agencies for information to dealing with blanket requests for all personal information about an individual.
>
> The costs associated with the systems, processes and labour, required to verify customer requests and retrieve the relevant data, has not been taken into account by Telstra in determining the cost impacts of the Data Retention Bill. Telstra does have the ability to charge customers for providing access to personal information, but we consider it a real risk that we would not be able to fully recover our costs in light of the Office of the Australian Information Commissioner's (OAIC) Australian Privacy Principles Guidelines on charging for access requests.[87]

Committee comment

6.127 In regards to personal access, the Committee notes Australian Privacy Principle 12 but considers that individuals should have an unambiguous right to access their personal telecommunications data retained under the mandatory data retention regime. The Committee recommends amendments to the Bill to clarify the right to access personal data retained under the data retention regime.

6.128 The Committee notes that telecommunications service providers are currently able to recover the cost under the *Privacy Act 1988* and considers that this model should apply to these arrangements.

---

86 Telstra, *Submission 112*, pp. 4-5.

87 Telstra, *Submission 112*, p. 5.

Recommendation 24

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to make clear that individuals have the right to access their personal telecommunications data retained by a service provider under the data retention regime. Telecommunications service providers should be able to recover their costs in providing such access, consistent with the model applying under the Privacy Act in respect of giving access to personal information.

Authorisation process for accessing historical telecommunications data

6.129 At a public hearing, the Attorney-General's Department confirmed that the Government does not intend to amend the existing authorisation process in the Bill:

> **MR DREYFUS**: …This bill—and if you can confirm—is not dealing in any way with the powers that there presently are for ASIO, the Australian Federal Police or other police forces to access telecommunications information. Is that right?
>
> **Ms Harmer**: The only amendment to the access arrangements is to reduce the number of agencies who can access the data, but the access thresholds are not changed.[88]

6.130 However, the Committee notes that a significant number of submissions have raised concerns with the adequacy of the existing authorisation process or expressed the view that additional safeguards are necessary in light of the proposed data retention regime.

6.131 The remainder of this chapter will examine the following issues raised in evidence in the context of the proposed data retention regime:

- whether a warrant issued by an independent body (or similar process) should be required to authorise access to telecommunications data;
- whether the statutory thresholds for access to historic telecommunications data should be adjusted;
- whether additional requirements for access should apply in respect of privileged or other sensitive communications;

88 The Hon Mr Dreyfus QC MP and Ms Anna Harmer, acting First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 17 December 2014, p. 8.

- whether additional requirements in respect of destruction of telecommunications data in the possession of agencies are required.

The current position

6.132 The Explanatory Memorandum provides an overview of the process for obtaining access to historical telecommunications data:

> The TIA Act establishes a process of authorisation for access to telecommunications data that requires senior management to authorise access to this data before it is disclosed to an agency. The authorisation process requires the authorised officer to consider the need for access to this information on a case-by-case basis in accordance with a prescriptive legal framework.[89]

6.133 In its submission, the Attorney-General's Department provided further detail on which officers may authorise disclosure under the existing internal authorisation process:

> 'Authorised officers' of enforcement agencies may authorise the disclosure of telecommunications data under the TIA Act. Authorised officer are defined in section 5 of the TIA Act to include the following:
>
> - i. the head of an enforcement agency; or
> - ii. a deputy head of an enforcement agency; or
> - iii. a person who holds an office or position in the enforcement agency that is covered by an authorisation in force under subsection 5AB(1).
>
> Under section 5AB of the TIA Act, an agency head may authorise, in writing, management offices or positions within their agency for the purposes of authorising access to telecommunications data.[90]

6.134 The Department also described the legislative thresholds that apply when officers of an organisation are considering telecommunications data access authorisations:

> Chapter 4 of the TIA Act sets out the mechanisms for ASIO and the enforcement agencies to authorise the disclosure of data for a variety of lawful purposes.
>
> Section 178 of the TIA Act allows an authorised officer of an enforcement agency to authorise a C/CSP to disclose historic telecommunications data if the disclosure is reasonably necessary for the enforcement of the criminal law …

89 Data Retention Bill, *Explanatory Memorandum*, p. 19.

90 Attorney-General's Department, Submission 27, p. 42.

> Section 178A of the TIA Act allows an authorised officer of a police force to authorise a C/CSP to disclose historic telecommunications data to assist in locating a missing person.
>
> Section 179 of the TIA Act allows an enforcement agency to authorise a C/CSP to disclose historic telecommunications data if the disclosure is reasonably necessary for the enforcement of law imposing a pecuniary penalty or for the protection of the public revenue …
>
> For all of the above disclosure authorisation powers, section 180F of the TIA Act requires an authorised officer to take the privacy impact into account when making any such authorisation.[91]

6.135 The authorisation process for ASIO is similar. The Director-General of Security, a Deputy Director-General of Security, or an approved ASIO officer may authorise access to historical telecommunications data where they are satisfied that the disclosure would be in connection with the performance by ASIO of its functions.[92]

6.136 In response to a request from this Committee to outline how the process of access works, the New South Wales Police Force (NSW Police) explained:

> All of our inspectors and above—we call them commissioned officers—…
>
> They are all authorised under the act—I think it is section 5AB. They are authorised officers to approve metadata requests under section 178 of the TIA act. They are in the field, say, at a particular location. Someone puts the request up to the inspector. They call in the boss. They discuss it—a particular crime has just been committed or is about to be committed—and there is a process in place. There will be discussion. There is a cost involved too. The constable or the detective will need to talk to the boss to make sure that everyone is happy, and costs will obviously be paid for the metadata. They look at the privacy aspects of the particular crime and the safeguards. There is a process on the computer called our 'I Ask' system. They log in online. They put down a narrative of the brief and so on. It goes through to the 'I Ask' system at Parramatta where it is approved. That system then talks to the carrier's system and it is vetted by 'I Ask', which is done by another inspector. There is more supervision and vetting, and the data is obtained from the carrier. At the local level, the inspector will approve that particular request. They will look at all the

91 Attorney-General's Department, Submission 27, p. 42.

92 *Telecommunications (Interception and Access) Act 1979*, section 175.

> safeguards, facts and circumstances to justify the request, and so on. It goes to 'I Ask'. There is another vetting process at 'I Ask', and then the carrier accesses the records back to the officer who requested the data under the process.…
>
> It is standardised, accounted, documented, recorded …[93]

Should a warrant from an independent authority be required?

6.137 A significant number of submitters have expressed the view that there is a need for an increase in procedural protections in respect of agency access to telecommunications data.

6.138 For example, in their submission, Professor Geroge Williams and Dr Keiran Hardy raised the following concern:

> We are concerned by the prospect that enforcement agencies will effectively be able to access metadata on a 'self-serve' basis. Given that metadata can reveal a significant amount of identifying information about an individual, we believe that greater procedural protections for accessing metadata should apply….
>
> This could be achieved through a warrant process along the lines of that allowing access to stored communications.…
>
> Metadata is not trivial information and enforcement agencies should not be free to access that information wherever doing so is reasonably necessary to enforce minor infringements, such as parking or library fines.[94]

6.139 The councils for civil liberties across Australia highlighted that, without prior oversight, any abuse of the legal parameters could only be detected after the fact. The councils argued the necessity of judicial oversight prior to access:

> The CCLS greatest concern about the proposed safeguards is the lack of prior oversight of the operation of enforcement agencies access to telecommunications meta-data …
>
> It is clearly unacceptable for the 'enforcement agencies' or ASIO to be their own authorisers of access to such personal information. Any oversight of their processes and detection of any abuse of the legal parameters could only be detected post hoc.
>
> There is an obvious and well tested, traditional safeguard that should be included in the bill. Access to both retrospective and prospective meta-data under the proposed scheme should only be

93 Detective Superintendent Arthur Kopsias, APM, Telecommunications Interception Branch, New South Wales Police Force, *Committee Hansard*, Canberra, 30 January 2015, pp. 58-59.

94 Professor Williams and Dr Hardy, *Submission 5*, p. 5-6.

> on the basis of a prior warrant authorisation from a judicial authority.[95]

6.140 The Committee notes that the Parliamentary Joint Committee on Human Rights also recommended use of a warrant:

> [T]he committee notes that the proposed oversight mechanisms in the bill are directed at reviewing access powers after they have been exercised. However, the statement of compatibility does not address the question of why access to metadata under the scheme should not be subject to prior review though a warrant system, as is the case for access to other forms of information under the TIA Act.
>
> The committee considers that requirements for prior review would more effectively ensure that the grant of access to metadata under the scheme would be consistent with the right to privacy.
>
> The committee therefore recommends that, so as to avoid the unnecessary limitation on the right to privacy that would result from a failure to provide for prior review, the bill be amended to provide that access to retained data be granted only on the basis of a warrant approved by a court or independent administrative tribunal, taking into account the necessity of access for the purpose of preventing or detecting serious crime and defined objective grounds.[96]

6.141 A number of submitters expressed their support for the Parliamentary Human Rights Committee recommendation. Blueprint for Free Speech recommended that any access to telecommunications data should be supported by a warrant on the terms set out by that Committee.[97] The Law Institute of Victoria noted the Human Rights Committee's recommendation and expressed the view that judicial oversight should be required. Mr Josh O'Callaghan referred to the Committee's recommendation and highlighted the protection warrants provide:

> I also have an issue with current system we have; which allows the warrantless access (without judicial oversight; under any circumstance) of the existing telecommunications networks.…
>
> By removing the process to obtain warrants, citizens are losing their right for judicial protection against corruption and abuse.[98]

---

95 Councils for civil liberties across Australia, Submission 129, pp. 15-16.

96 Parliamentary Joint Committee on Human Rights, *Fifteenth Report of the 44th Parliament*, p. 18.

97 Blueprint for Free Speech, *Submission 54*, p. 14.

98 Mr Josh O'Callaghan, *Submission 29*, p. 1.

6.142 The Australian Human Rights Commission recommended in its submission that an independent authorisation system by a court or administrative body be implemented. As with a number of other submitters, the Commission noted that access to telecommunications data may not be any less intrusive than access to content:

> The current regime allows agencies to access communications data without a warrant but mandates a warrant for access to the content of communications. The Commission considers that a warrant system is necessary for the access to communications data as well. This is especially the case given the question of whether the distinction between content and communications data for the purposes of the right to privacy can be legitimately maintained …
>
> Contrary to the claims made in the Explanatory Memorandum, the Commission considers the retention of and access to communications data may not be any less intrusive than retention of and access to content. The requirement to store communications data on each and every customer just in case that data is needed for law enforcement purposes is a significant intrusion on the right to privacy and justifies a warrant system for access to it.[99]

6.143 The Commission also referred to international precedent for use of warrants to access telecommunications data:

> The Commission notes that the Court of Justice of the European Union considered that an independent administrative or judicial body should make decisions regarding access to the retained communications data on the basis of what is strictly necessary …
>
> Further, requiring a warrant to access metadata is not without precedent in other countries. In the EU, eleven Member States require judicial authorisation for each request for access to retained data. In three Member States judicial authorisation is required in most cases. Four other Member States require authorisation from a senior authority but not a judge.[100]

6.144 In its submission, the Commission noted the safeguards that apply under the existing legislation and the Bill, but expressed the concern that they only apply after a power has been exercised.

> While these safeguards are important checks on the scheme, they are all directed at reviewing access powers after they have been exercised. The Commission considers that a warrant or authorisation system for access to retained data by a court or

99 Australian Human Rights Commission, *Submission 42*, p. 11.

100 Australian Human Rights Commission, *Submission 42*, pp. 10-11.

> administrative body provides a more effective safeguard to ensure that the right to privacy is only limited where strictly necessary.[101]

6.145 Australian Lawyers for Human Rights explained why, in its view, a warrant to access telecommunications data is necessary:

> Today, warrants should be required to access metadata so that (1) individuals may not be investigated by government bodies without proper cause, and so that (2) an appropriate check or balance is applied through the mechanism by which the warrant is obtained from the courts.
>
> To remove the requirement for prior authorisation via a warrant is to undermine both democracy and the rule of law by reducing the checks and balances essential to a democratic system.[102]

6.146 The Human Rights Law Centre expressed the view that a warrant or other prior approval process is necessary, and also expressed the need for a notification and review mechanism:

> A warrant or other similar prior approval process is necessary to ensure that issues of privacy are considered by an independent authority and that there is sufficient evidence to avoid a fishing expedition …
>
> The absence of a warrant or other independent authorisation process prior to access and use of the stored data gives rise to serious concerns regarding the propriety, and apparent propriety, of the access and use …
>
> A warrant or similar prior approval process should also provide a mechanism for individuals to be notified and have the opportunity to challenge the legality of access to their telecommunications data. Notification could occur after access where ex parte approval was necessary for law enforcement or national security purposes. This process should mitigate the concern that the right to an effective remedy is being impermissibly interfered with because individuals are unable to challenge decisions or applications in relation to their stored metadata because they are never informed of the decisions or applications.[103]

6.147 The Parliamentary Human Rights Committee similarly recommended a requirement for individuals to be notified that their data has been subject

---

101 Australian Human Rights Commission, *Submission 42*, p. 12.

102 Australian Lawyers for Human Rights, *Submission 88*, p. 7.

103 Human Rights Law Centre, *Submission 71*, p. 8.

to an application for authorisation to access, and recommended a process to allow individuals to challenge such access.[104]

6.148 Mr Scott Millwood strongly advocated for the use of a targeted warrant system for accessing telecommunications data:

> While oversight provisions are a welcome inclusion in the Bill, an oversight function by the Commonwealth Ombudsman is not comparable with the meaningful judicial oversight provided by the targeted warrant system. This submission recommends that serious consideration be given to ensuring access to metadata is governed by a warrant system, in which judicial consideration can be given to the requirements of necessity and proportionality. This would simultaneously address the requirement of a legal avenue for remedy for victims of violations of their rights to privacy under the data retention regime.[105]

6.149 Mr Millwood also noted the risk of telecommunications data being used for political purposes, a concern that was reflected in a number of submissions to this inquiry:

> The hard truth is, systems of mass surveillance are inevitably used to target political opposition. It is conceivable that use or misuse of an individual's metadata could cause great damage to an individual's right to freedom of expression and right to participate in Australian public life.[106]

6.150 Guardian Australia similarly expressed its concerns with the lack of a pre-disclosure independent oversight mechanism for access to telecommunications data, and also proposed the use of a public interest monitor in such a process:

> Guardian Australia submits that it is reasonable for the public to expect that authorisation from an independent, appropriately qualified person ought to be required before metadata is accessed. Independent authorisation is such a commonly occurring feature of the safeguards used by democratic societies in the context of surveillance schemes that the Committee is requested to investigate further, to test seriously the agencies' claims about cost in time and money, and to recommend an appropriate process for independent authorisation prior to access.
>
> … The Committee is requested to recommend the creation of an independent Public Interest Monitor role. A suitably qualified and

104 Parliamentary Joint Committee on Human Rights, *Fifteenth Report of the 44th Parliament*, p. 21.

105 Mr Millwood, *Submission 121*, p. 14

106 Mr Millwood, *Submission 121*, p. 16.

> experienced person should have the primary function of testing the arguments of agencies which seek to conduct surveillance and of articulating the privacy and others interests which ought to be weighed by the decision-maker.[107]

6.151 The Australian Privacy Foundation and the councils for civil liberties across Australia also expressed support for a public interest monitor in the context of a warrant or similar process.[108]

6.152 In response to suggestions that a warrant regime should be used, law enforcement and security agencies noted the existing protections and safeguards that apply and raised significant concerns in respect of the impact such a requirement would have on their operations.

6.153 The AFP explained its concerns with a warrant requirement to access telecommunications data in its submission:

> The AFP considers that, given the existing safeguards, constraints and processes governing the authorisation regime, and the extended oversight provisions under the Bill, that a warrant scheme for access to telecommunications data would not significantly improve accountability or transparency of the scheme. Rather, the AFP considers that such a scheme would generate unnecessary administrative burden and costs on both agencies seeking access to telecommunications data and on the issuing authority for such warrants.
>
> 32. The AFP is concerned that the time (not even counting the financial cost) required per request to prepare and progress a warrant for telecommunications data would reduce operational responsiveness in time sensitive cases and create a bureaucratic burden, diverting investigative resources from the field. The AFP conservatively estimates, based on other warrant applications that the process for preparing such a warrant would take at least 8 hours of dedicated work. Extending this to the existing rate of requests for telecommunications data, this would equate to a requirement for over 100 staff to be solely committed to warrant preparation duties.
>
> 33. A scheme requiring agencies to obtain a warrant for historical telecommunications data would also create a significant additional burden on the already stretched Administrative Appeals Tribunal and judicial system, who would be required to consider

107 Guardian Australia, *Submission 132*, pp. 12-13.

108 Australian Privacy Foundation, *Submission 75*, p. 3; Councils for civil liberties across Australia, *Submission 129*, p. 16.

> approximately 25,000 applications from the AFP alone every year.[109]

6.154 In its submission, ASIO explained its concerns with a warrant mechanism, and also noted the extensive safeguards that currently apply:

> ASIO's concern with implementing a warrant regime for data access is its impact on our operational response and agility: the significant bureaucratic overlay such a scheme would impose and the consequential delay in assessing and responding to emerging security threats before they are realised.[110]

6.155 At public hearing, representatives of New South Wales, South Australia and Victoria police forces explained to the Committee how metadata is used and the impact a warrant process could have on their operations. South Australia Police stated:

> Metadata is really just about where the communication occurred, when it occurred, place, time—those sorts of issues. As you quite rightly say, it does not actually relate to the content of that metadata. Often, when we seek that metadata, we are just looking for information because we do not really have much else to go on. We are using that information tool to find out what contact, what communication, the suspects or the victim have had and to then go and speak to those individuals to find out what is the relationship and just going through that process, as any good investigator should do. Really it is an intelligence tool to provide us with information to assist us with that investigation. Often the metadata does not get us anywhere because it is not relative to the investigation.[111]

6.156 The NSW Police noted the impact a warrant regime could have:

> [T]he first 24 hours in a homicide investigation is critical, a significant time delay to go under a warrant regime would significantly impact on both the effectiveness and certainly the efficiency of criminal investigations …
>
> I would say the balance at the moment is quite appropriate in terms of metadata. As I said, internally there are checkpoints that we need to go through to get there. There is external oversight—and I can have Superintendent Kopsias talk in terms of the telecommunications interception act and Ombudsman, Commonwealth and state, oversighting. In the initial stages of an

109 AFP, *Submission 7.1*, pp. 12-13.

110 Australian Security Intelligence Organisation, *Submission 12.1*, p. 48.

111 Assistant Commissioner Dickson, *Committee Hansard*, Canberra, 30 January 2015, p. 45.

> investigation, it is really about gathering information as quickly as we can so we can try to narrow down suspects, try to identify communications and found the investigation and the direction we are going to go with it. If a significant layer of bureaucracy is put on top of that, that will significantly impede investigations. I would think that they are appropriate, and I certainly take note of Mr Byrne's comments before. But when you look at the significant number of inquiries that are made for metadata each year and the way that they are handled compared to the response we do get from both the state and Commonwealth Ombudsman, I think we have the processes very appropriate.[112]

6.157 NSW Police added this further comment on the potential impact of a warrant regime:

> From a New South Wales Police Force prospective, the volume of our metadata requests if we put a warrant regime on top of the metadata scheme would—I will make a bold statement—virtually cripple our organisational capacity to effectively deal with organised crime and serious crime. I would make that statement to you. It is not just responding during business hours; it is also after hours. We respond to kidnappings and other serious crime after hours and on weekends. You would need after-hours people to do that type of work. Just the sheer volume of metadata and TI requests would hamper our investigative capacity.
>
> In terms of oversight, I do not think a warrant scheme would add more to due diligence and to the accountability and oversight process currently in place at the moment. As Mr Lanyon told you, we have enough internal processes and accountability schemes in place to ensure governance and equitable practices are adhered to at all times in compliance with the legislative practices that we adhere to.[113]

6.158 Victoria Police added:

> [I]f we were to move to a judicial warrant situation for metadata, one of the things I think it would throw up in terms of an anomaly is that telecommunications interception warrants, by definition, require metadata within the applications—and quite a deal of metadata—to substantiate the application. We would effectively be moving to a situation where, in a lot of instances, we would

112 Assistant Commissioner Malcolm Lanyon APM, New South Wales Police Force, *Committee Hansard*, Canberra, 30 January 2015, pp. 46, 47.

113 Detective Superintendent Arthur Kopsias APM, New South Wales Police Force, p. 47.

> need a warrant to obtain the information that we would need to obtain the warrant. I think that would raise a whole range of issues as well.[114]

6.159 A number of submitters did not accept agency concerns regarding the impact of a warrant requirement on the ability to perform their functions. The councils for civil liberties across Australia submitted:

> The CCLS do not accept the argument that having to access a warrant will impose an unmanageable administrative burden on the agencies or ASIO. The warrant process provides an important procedural safeguard without any great inconvenience. Such inconvenience and administrative burden that does accompany it, is a reasonable and necessary trade-off for such significant intrusion into the privacy rights of the community.[115]

6.160 The Law Council of Australia acknowledged that an increase in warrant applications would result, but considered that this would cause agencies to only apply for access in cases when an interference with privacy was considered necessary:

> The Law Council understands that there are concerns that a warrant-based system would limit the ability of law enforcement and national security agencies to employ what is often the lowest risk, least resource-intensive and least intrusive investigative tool. The Law Council does not agree that the method of access to retained communications should be the paramount consideration. Rather, protection and oversight of rights of privacy should be paramount …
>
> The Law Council acknowledges that a warrant-based system for access to telecommunications data would increase the number of warrant applications. However, it would serve as an important deterrent for agencies to only apply for access when an interference with privacy is considered necessary.
>
> The Law Council rejects the argument that, even if accompanied by increased resourcing, a warrant regime would distort the ability of issuing authorities to perform their day-to-day functions as members of the judiciary or AAT. This is an issue of adequate resourcing of the Courts and the AAT. The government has a responsibility to sufficiently resource those bodies charged with supervision of such activities to ensure that rights of privacy are not unnecessarily infringed upon.

---

114 Inspector Gavin Segrave, Victoria Police, *Committee Hansard*, Canberra, 30 January 2015, p. 49.

115 Councils for civil liberties across Australia, *Submission 129*, p. 16.

6.161 In response, the Attorney-General's Department provided a number of reasons why it did not consider a warrant regime appropriate:

> The benefits of introducing a warrant regime would be outweighed by the impact on agencies' ability to combat serious crime and protect public safety. Timely access to telecommunications data can provide agencies with vital leads before evidence can be lost or destroyed. However, warrant applications are resource intensive, and can take days, if not weeks, to prepare and complete. Delaying an agency's ability to begin an investigation by this length of time would seriously harm their ability to investigate crimes or threats to national security.
>
> Telecommunications data is used most commonly in the early stages of an investigation, when evidence is at risk of being lost, or where victims might be in imminent risk of danger. For example, a police force investigating a suspected kidnapping would often begin their investigation by seeking information about whom the victim had been communicating with immediately prior to their kidnapping. Early information about the whereabouts of the victim would increase the chances of a successful rescue.
>
> Warrants are also typically reserved for the most intrusive powers, such as the power to enter a home, intercept phone calls, or access stored communications. Many information-gathering powers that are exercised by agencies under Commonwealth, State and Territory laws do not rise to that level of intrusiveness and may be exercised without a warrant. Examples of such powers are powers to obtain banking, financial and healthcare records. The power to access data is only of the same level of intrusiveness as these powers. Non-warranted access to information is a normal part of any law enforcement framework.
>
> Furthermore, to require a warrant in this circumstance would be counterintuitive to the fundamental tenet of proportionality because telecommunications data serves to establish the case for more intrusive powers to be deployed under a warrant.

6.162 The Attorney-General's Department also noted that precedent for non-warranted access to information is found in a number of areas within the existing Australian legal system:

> [W]hile there are warrants for access to some types of information and tools, warrants are typically reserved for those tools that are most intrusive. The committee has already commented today on telecommunications interception warrants, but there are a range of other warrants for more intrusive steps—search warrants et cetera.

> However, access under alternative mechanisms is certainly by no means unprecedented. Indeed, it is common through 'notice to produce' authorisation processes et cetera to access more routine ranges of information that are less intrusive. Telecommunications data, as we said, is a basic data point. It is typically used at the beginning of investigations to commence inquiries, to identify inquiries and to pursue those. It is a relatively less intrusive range of information. It is also often required to progress investigations quickly and to provide the information that is then required to support something like an interception warrant. So it then supports warranted access to other tools.[116]

6.163 Professor Williams and Dr Hardy acknowledged the significant administrative burden of a judicial warrant process and proposed a ministerial warrant process as an alternative.

> We accept that a warrant process along these lines could pose a significant administrative burden to law enforcement and intelligence agencies investigating serious criminal offences and threats to national security. As such, a preferable alternative might be to implement a ministerial warrant process. This could be incorporated into existing ministerial warrant processes where available to ensure maximum efficiency without compromising procedural safeguards …
>
> A ministerial warrant process would allow law enforcement and intelligence agencies to access metadata in a timely fashion whilst ensuring that there is enhanced political accountability for the regime.[117]

6.164 Appearing before the Committee, Professor Gillian Triggs, President of the Australian Human Rights Commission, acknowledged the issues with the imposition of a warrant process and suggested some more nuanced administrative process should be adopted:

> We suggest that some form of administrative—possibly judicial but for practical purposes administrative—body be developed in advance of the access or collection process so that there is some form of control … If it is accepted that a warrant is necessary for content, I think it at least has to be further explored why it is not necessary to have a warrant at the beginning of the process.
>
> Again, I am conscious of the concerns that the warrant process can be time consuming, expensive and difficult to establish, and that is

116 Ms Harmer, *Committee Hansard*, Canberra, 17 December 2014.

117 Professor Williams and Dr Hardy, *Submission 5*, p. 6.

> very important when we are dealing with critical questions of life and serious criminal offences. So we would suggest that, rather than going necessarily through a warrant process, some more nuanced process of administrative authorisation be adopted which is simpler, clearer and cleaner …[118]

6.165 The Attorney-General's Department referred to the use of generic warrants in some European jurisdictions, but noted the United Kingdom's Interception of Communications Commissioner's concerns in respect of how proportionality can be judged properly under such schemes, and expressed concern that use of a generic warrant may result in important checks being removed:

> The Australian scheme is comparable to that which exists in the UK where a disclosure of information to be sought individually which allows the proportionality of each particular disclosure to be considered separately. This is required by section 180F of the TIA Act, which provides that authorising officers must have regard to whether any interference in the privacy of any person or persons that may result from a particular disclosure is justifiable, having regard to the likely relevance and usefulness of the information and the reason why the disclosure or use is proposed to be authorised.
>
> Those considerations are important checks that would possibly be lost from the investigative process if 'generic' whole-of-investigation warrants were to be adopted. The checks may be lost as the issuing authority would be required to decide whether or not to authorise disclosure of information without knowing the relevance of particular pieces of information to an investigation or the privacy impact of any such disclosures.
>
> The Department's view is that the current law and policy settings in the TIA Act are preferable, as they require the person authorising the disclosure of this basic investigative material to turn their mind to privacy and proportionality considerations when deciding whether or not to authorise particular disclosures.[119]

6.166 The Australian Privacy Commissioner had considered a 'generic' warrant and concluded in his submission that it would not be effective:

---

118 Professor Gillian Triggs, President, Australian Human Rights Commission, *Committee Hansard*, Canberra, 29 January, p. 71.

119 Attorney-General's Department, *Submission 27*, p. 19.

> There has also been discussion of an alternative requirement for enforcement and security agencies to obtain a 'generic' warrant to access telecommunications data. This was discussed at the hearing on 17 December 2014, where an example was given of a warrant to authorise access to telecommunications data for all terrorism investigations. I do not consider that such a generic warrant regime (as discussed at the hearing) would provide the necessary level of scrutiny to be effective to increase the current level of oversight of the disclosure of telecommunications data.[120]

6.167 In a supplementary submission, the Commissioner also considered the issue of additional safeguards that might be introduced for the use of telecommunications data for more minor crimes. The Commissioner proposed three alternatives, the first being the introduction of a warrant, and the second being a more restricted warrant regime applying in relation to minor offences:

> An alternative to introducing a blanket warrant requirement, could be an amendment to Chapter 4 of the TIA Act to require enforcement agencies to obtain a warrant where access to telecommunications data is sought in relation to the investigation of an offence other than a 'serious contravention', as defined in s 5E of that Act.
>
> While the requirement to obtain a warrant in relation to minor offences may appear counterintuitive, such an approach would recognise the urgency of requests for telecommunications data necessary for the investigation of serious offences and threats to national security. This is also in-keeping with the intention of the proposed data retention scheme, which has focused on the need to ensure that Australian enforcement and security agencies have access to the information they require to combat such serious offences and threats.[121]

6.168 The third alternative suggested by the Commissioner was amending section 180F of the TIA Act to require authorised officers to have regard to additional factors:

> [T]he Bill could amend s 180F of the TIA Act to explicitly require an authorised officer to have regard to the following additional factors:
>
> - the seriousness of the offence,

120 Office of the Australian Information Commissioner, *Submission 92*, p. 20.

121 Office of the Australian Information Commissioner, *Submission 92.1*, p. 3.

- whether there are any other reasonable methods of investigating the offence, that do not involve the use of telecommunications data, available to the enforcement agency, and
- the likely impact on the community of the enforcement agency not being able to access the relevant telecommunications data.[122]

6.169 During a public hearing, the Committee asked Professor George Williams and Dr Keiran Hardy whether the Single Point of Contact (SPoC) mechanism, as used in the United Kingdom, would be a useful safeguard to include in the Data Retention Bill. In a supplementary submission, Professor Williams and Dr Hardy outlined the scheme and expressed the view that it would not resolve issues of external oversight.

> A SPoC is an accredited individual (or group of individuals) in a public authority who acts as a 'gatekeeper' before requests for communications data are submitted to a senior authorising officer.
>
> For example, if a junior police officer wanted to access communications data under Part 1, Chapter 2 of the Regulation of Investigatory Powers Act 2000 (UK), he or she would first submit an application to the SPoC. The SPoC would then consider the merits and lawfulness of that request, and provide advice on its drafting, before sending it to a senior designated officer to be authorised.
>
> We believe that such a scheme could be a useful addition to the Bill currently before the Committee, but it would not resolve the Bill's major issues. A SPoC regime would not add any external oversight or political accountability to the proposed data retention regime, as it would operate internally within enforcement agencies and criminal law enforcement agencies. It would also not resolve other key issues raised by the Bill, such as whether local councils should have access to metadata for the purpose of enforcing fines and the like. We believe that the government should focus on resolving these key issues in the primary legislation.[123]

Committee comment

6.170 A number of submitters raised concerns regarding the authorisation process for access to telecommunications data. In particular some submitters argued that access to telecommunications data is no less

122 Office of the Australian Information Commissioner, *Submission 92.1*, pp. 3-4.

123

intrusive than access to the content of telecommunications, and consequently that the same pre-access approval processes should apply.

6.171 The Committee acknowledges that in some circumstances access to telecommunications data can represent a significant privacy intrusion. However, the Committee notes the evidence provided that telecommunications data and telecommunications content are not used in the same way by law enforcement and security agencies, and does not consider that the same authorisation processes must necessarily apply. However the Committee has paid particular attention to assessing the adequacy of existing safeguards and oversight mechanisms for authorisation of access to telecommunications data.

6.172 The formulation of safeguard and oversight mechanisms in this context requires a careful balancing of competing public interests – maximising accountability, integrity and protection of liberty while minimising adverse impacts on both the ability and the agility of agencies to perform their legitimate functions of enforcing the law and safeguarding the Australian community.

6.173 During the conduct of this inquiry, the Committee has received compelling evidence that the introduction of a warrant process (judicial or ministerial) for access to telecommunications data would significantly impede the operational effectiveness of agencies and that this would be to the detriment of the protection of the Australian community. The Committee was not convinced that a 'generic' warrant would be a suitable alternative.

6.174 After close consideration of the evidence, the Committee concludes that the existing internal authorisation regime contained in the TIA Act is appropriate, noting the other safeguards and oversight mechanisms that apply.

Thresholds for authorising access to telecommunications data

6.175 Some submitters raised concerns that the threshold for authorising access to telecommunications data is not proportionate to the level of privacy intrusion that may arise under the regime. Some proposed that the thresholds for agencies to access telecommunications data should be amended to include a requirement as to the gravity of the offence/security matter being investigated. For example, the Australian Privacy Foundation stated in its submission that it considers there is a strong case for applying the current threshold for accessing content to agency access to telecommunications data:

> Given the extent to which access to telecommunications data my interfere with the right to privacy just as much as access to

> communications content, the APF consider there is a strong case for introducing a uniformly high threshold for access to both communications content and telecommunications data.[124]

6.176 The Law Institute of Victoria recommended that access to telecommunications data be restricted to criminal law enforcement agencies for preventing, detecting or prosecuting serious crimes. In reaching this conclusion the Institute stated:

> This Bill does not refer to 'serious crime'. There are no criteria which would ensure that data is only accessed or used for purposes of prevention, detecting or prosecuting serious crime or even matters that constitute criminal offences. The Bill goes beyond a legitimate purpose. The agencies that can be classified as 'enforcement agencies' can access data related to their function of enforcing offences that impose pecuniary penalties and/or protect public revenue.[125]

6.177 The Australian Human Rights Commission noted the Court of Justice decision in respect of the EU Data Retention Directive, and concluded that access to historical telecommunications data should be limited to sufficiently serious crimes:

> As outlined above, the Court of Justice of the European Union found that the EU Data Retention Directive was not a proportionate interference with the right to privacy. One of the reasons for this was that it considered that access and use of the data should be restricted to the prevention, detection or prosecution of defined, sufficiently serious crimes.
>
> The Commission considers that access to communications data should be restricted to sufficiently serious crimes to warrant the intrusion on the right to privacy.[126]

6.178 The Parliamentary Joint Committee on Human Rights, in its review of the Bill, recommended changes to the existing authorisation scheme to address concerns in respect of the existing threshold for access to telecommunications data:

> The lack of a threshold, relating to the nature and seriousness of the offence, for access to retained data appears to be a disproportionate limitation on the right to privacy. The committee considers that to ensure a proportionate limitation on the right to privacy, an appropriate threshold should be established to restrict

124 Australian Privacy Foundation, *Submission 75*, pp. 24-25.

125 Law Institute of Victoria, *Submission 117*, p. 12.

126 Australian Human Rights Commission, *Submission 42*, p. 9.

> access to retained data to investigations of specified threatened or actual crimes that are serious, or to categories of serious crimes such as major indictable offences (as is the current threshold for requiring the option of trial by jury). The committee is additionally concerned that the threshold of 'reasonably necessary' for the enforcement of offences may lack the requisite degree of precision.
>
> The committee therefore recommends that the bill, so as to avoid the disproportionate limitation on the right to privacy that would result from disclosing telecommunications data for the investigation of any offence, be amended to limit disclosure authorisation for existing data to where it is 'necessary' for the investigation of specified serious crimes, or categories of serious crimes.[127]

6.179 A number of submitters to this inquiry support the Parliamentary Human Rights Committee's recommendation. For example, the Victorian Commissioner for Privacy and Data Protection stated:

> The Bill should be amended to include clearly defined objective thresholds for access to retained data by criminal law enforcement agencies. These thresholds should be set taking into account the public interest, including consideration of the principles of proportionality, necessity, effectiveness, and transparency. Access should only be available in relation to serious offences, for example, offences that attract significant periods of imprisonment. The PJCHR recommendation to limit disclosure authorisation for existing data to where it is necessary for the investigation of specified serious crimes, or categories of serious crimes is supported.[128]

6.180 The Human Rights Law Centre noted the Human Rights Committee's recommendation and added:

> The failure to set out objective criteria restricting access and use of data for the purpose of preventing and detecting carefully defined serious offences or of conducting criminal prosecutions was one of the key criticisms levelled at the Directive in the Digital Rights decision.
>
> The same criticism was raised in Germany in relation to legislation intended to implement the Directive into German law. The legislation was found to be disproportionate and unconstitutional, in part because the stored data could be accessed for a wide

127 Parliamentary Joint Committee on Human Rights, *Fifteenth Report of the 44th Parliament*, p. 16.

128 Commissioner for Privacy and Data Protection (Victoria), *Submission 39*, p. 7.

> variety of purposes, rather than strictly for the investigation of serious crimes.
>
> The Bill should establish a gravity threshold so that retained metadata can be accessed and used only where it is necessary for investigating serious crimes; not minor or trivial offences.[129]

6.181 The Muslim Legal Network (NSW) expressed the view that access to data should be restricted to investigations of terrorism related offences only:

> [W]e strongly believe that not only should the type of enforcement agencies that can access retained data be restricted, but the purpose of accessing the retained data should be limited to the investigations of terrorism related offences only. The overriding rationale of data retention, if it is to be accepted into Australian law, should be one of targeted surveillance and not mass surveillance. Mass surveillance is ineffective, disproportionate and a woefully inadequate response to the threat of terrorism.[130]

6.182 In its submission the Attorney-General's Department highlighted the importance of access to telecommunications data for all investigations, serious or otherwise:

> Telecommunications data is critical to the investigation of almost any criminal activity, serious or otherwise, and almost any activity prejudicial to security that has been facilitated, enabled or carried out via communications technology. For online investigations, telecommunications data is, in many cases, the primary form of information used by law enforcement agencies to identify, investigate, prevent and prosecute these serious crimes and threats to national security. It is used in almost all national security investigations conducted by the Australian Security Intelligence Organisation (ASIO), including almost all counter-terrorism, espionage and intelligence investigations, and all cyber-security investigations.
>
> Telecommunications data can provide important leads for agencies, including evidence:
>
> - of connections and relationships between persons of interest
> - of suspects' movements and behaviours
> - of events immediately before and after a crime, and
> - to exclude people from suspicion.
>
> Telecommunications data is also foundational information required as a necessary precondition to more intrusive

129 Human Rights Law Centre, *Submission 71*, p. 10.

130 Muslim Legal Network (NSW), *Submission 198*, p. 10.

> investigative tools such as access to stored communications and telecommunications interception. Conversely, it is always desirable to rule innocent parties out from suspicion as early as possible, both to prevent any unnecessary intrusion on their privacy, and to ensure that scarce investigative resources are used efficiently. While all investigative techniques involve some degree of intrusion, the use of telecommunications data is one of the least privacy intrusive investigative tools available to agencies.[131]

6.183 The Department noted restricting access to 'serious crime' would have 'an unquantified impact on the investigation of crime types that agencies' currently have the capabilities to investigate'.[132]

6.184 The Department also explained its view that introduction of a threshold for access to telecommunications data based on the seriousness or gravity of an offence would be in contravention of the Cybercrime Convention:

> As a party to the Council of Europe Convention on Cybercrime, Australia has international obligations to make access to telecommunications data available for the investigation of all criminal offences. Article 14(2) of the Cybercrime Convention requires parties to ensure that telecommunications data is available for the investigation of any criminal offence, not just serious offences. Accordingly, amendments that reduce the number of agencies that have access to telecommunications data based on the gravity of the conduct in question would contravene Australia's obligations under the Convention. However, Australia's obligations under the Cybercrime Convention do not preclude reducing the range of agencies that have access to data, because Australia's obligations under the Cybercrime Convention relate only to the availability of telecommunications data for all offences, without specifying the range of agencies which must have access to such data.[133]

6.185 At a public hearing the Australian Privacy Commissioner noted that in his submission he had proposed that the Bill be amended to limit the purposes for which telecommunications data can be used and disclosed to the investigation of serious crime and threats to national security. However, the Commissioner went on to revise his position, noting the Attorney-General's Departments advice in respect of the application of the Cybercrime Convention:

---

131 Attorney-General's Department, *Submission 27*, p. 5.

132 Attorney-General's Department, *Submission 27.2*, p. 5.

133 Attorney-General's Department, *Submission 27*, p. 42.

> [S]ince lodging that submission, I note that the Attorney-General's Department has suggested that to meet Australia's obligations under the Council of Europe's cybercrime convention access to telecommunications data cannot be limited in this way. If that is the case then I consider that further thought needs to be given to what additional safeguards might be put in place when access is for the purpose of the investigation of minor offences.[134]

6.186 Subsequent to the hearing, the Commissioner provided a supplementary submission in which he set out a number of suggestions for additional safeguards that might be put in place. This included implementation of a warrant regime, or amending section 180F of the TIA Act to require an authorised officer to have regard to the seriousness of the offence and the likely impact on the community of the enforcement agency not being able to access telecommunications data for the investigation of that offence.[135]

Committee comment

6.187 The Committee has considered very carefully the views expressed that telecommunications access should be limited to sufficiently serious matters, such as serious contraventions of the law or serious national security issues.

6.188 The Committee notes that the level of intrusion into privacy incurred by accessing telecommunications data will vary depending on the particular circumstances, including the nature and volume of the telecommunications data accessed. The Committee also notes the complexities in balancing the competing public interests of individual privacy with enforcement of the law and protection of national security.

6.189 On balance, the Committee considers that the requirement in section 180F should be replaced with a more stringent requirement for the authorising officer to be satisfied on reasonable grounds that the particular disclosure or use of telecommunications data being proposed is proportionate to the intrusion into privacy.

6.190 In making this decision, the authorising officer should have regard to a list of specified factors, including the gravity of the conduct being investigated, the reason why the disclosure is proposed to be authorised, and the likely relevance and usefulness of the information to the investigation.

---

134 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, Canberra, 29 January 2015, p. 47.

135 Office of the Australian Information Commissioner, *Submission 92.1*, pp. 1-4.

6.191 A similar requirement should apply in respect of authorisations made by ASIO officers. The Committee notes that this could be achieved by appropriate amendments to the mandatory guidelines issued to ASIO by the Attorney-General.

6.192 The Committee also considers that enhanced accountability and oversight in respect of agencies' authorisation powers are necessary to provide reassurance to the Parliament and the community, and has addressed this further in Chapter 7.

Recommendation 25

The Committee recommends that section 180F of the *Telecommunications (Interception and Access) Act 1979* be replaced with a requirement that, before making an authorisation under Division 4 or 4A of Part 4-1 of the Act, the authorised officer making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate.

In making this decision the authorised officer should be required to have regard to:

- **the gravity of the conduct being investigated, including whether the investigation relates to a serious criminal offence, the enforcement of a serious pecuniary penalty, the protection of the public revenue at a sufficiently serious level or the location of missing persons;**
- **the reason why the disclosure is proposed to be authorised; and**
- **the likely relevance and usefulness of the information or documents to the investigation.**

Protection of client legal privilege and journalist sources

6.193 A number of submitters expressed significant concerns with agencies accessing privileged or otherwise sensitive telecommunications data.

6.194 The Law Institute of Victoria raised concerns that the Bill lacks safeguards to protect confidential and privileged information:

> The Bill contains no safeguards to protect confidential and privileged information, such as communications subject to client legal privilege, health records and journalists' sources. The lack of

such safeguards was one of the flaws highlighted by the CJEU in assessing the EU Data Retention Directive:

> *… it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.*

As illustrated above, telecommunications data is capable of revealing substantial information, and this could include information about communications between a lawyer and their client. For example, information exchanged by email or calls about potential witnesses between the lawyer and associates of the client, experts or other relevant parties, could disclose a defence case. A litigation strategy or case theory could be identified based on witnesses or experts contacted by the lawyer.

The Bill should contain specific safeguards to prevent disclosure of potentially privileged and confidential information. This issue could be taken into account as part of the warrant process and may in appropriate circumstances give an individual an opportunity to challenge access on the basis of privilege.

6.195 Mr Brian Ridgway noted his concern with the lack of an exception for professional privilege:

> The Bill makes no provision for the exception of professional privilege so that metadata associated with:
>
> - lawyers and their clients
> - doctors and their patients
> - journalists and their contacts
> - Members of Parliament and their correspondents
>
> will be able to be collected, accessed and analysed along with everything else.[136]

6.196 The Law Council of Australia noted that:

> although telecommunications data alone may not reveal the content or substance of lawyer/client communications, it would, at the very least, be able to provide an indication of whether:
>
> - a lawyer has been contacted;
> - the identity and location of the lawyer;
> - the identity and location of witnesses;
> - the number of communications and type of communications between a lawyer and a client, witnesses and the duration of these communications.[137]

136 Mr Brian Ridgway, *Submission 20*, p. 4.

137 Law Council of Australia, *Submission 126*, p. 20.

6.197 The Council emphasised the fundamental importance of client legal privilege, and concluded that:

> where access to retained data is sought relating to a lawyer's communications, it is essential that agencies seeking access demonstrate how privileged and confidential communications will be protected before a warrant can be issued and that sanctions for non-compliance be included.[138]

6.198 The Council also expressed the view that the scheme's application to other relationships whose communications are subject to the obligation of professional confidentiality regimes needs to be reconsidered, and made two recommendations in respect of privileged or sensitive data:

- Where access to retained data is sought for persons with legal obligations of professional confidentiality, there should be a requirement for agencies seeking access to demonstrate how privileged and confidential communications will be protected before a warrant can be issued.
- The TIA Act should include a legislative presumption that will ensure notice to lawyers and journalists in all but the most exceptional cases where access to retained telecommunications data is sought.[139]

6.199 In response to concerns in respect of client legal privilege, the Attorney-General's Department noted that:

> At common law, legal professional privilege attaches to the content of privileged communications, not to the fact of the existence of a communication between a client and their lawyer (See: *National Crime Authority v S* [1991] FCA 234). This distinction is demonstrated in the routine practice of parties to proceedings filing affidavits of documents listing documents in their possession that are not being produced on the ground of privilege, thereby disclosing the fact of the existence of the document…[140]

6.200 The Department further noted the statutory restrictions preventing the accessing of content under the telecommunications data access regimes, and concluded:

> As such, the data retention regime, and agencies' powers to access telecommunications data more broadly, do not affect or authorise the disclosure of the content of any communication, including any privileged communication.[141]

138 Law Council of Australia, *Submission 126*, p. 22.

139 Law Council of Australia, *Submission 126*, p. 23.

140 Attorney-General's Department, *Submission 27*, p. 21.

141 Attorney-General's Department, *Submission 27*, p. 21.

6.201 The Media, Entertainment & Arts Alliance (MEAA) expressed concerns, shared by a number of other submitters, that the proposed data retention regime would have a significant impact on the freedom of the media to perform its role:

> MEAA believes that any moves to increase the level of surveillance of journalists and their sources by intrusive means such as the data retention proposed in the Bill will harm the ability of journalists to scrutinise the powerful and hold them to account, to expose corruption, to champion and campaign for important issues, and to gain the trust of our audience and our sources.[142]

6.202 MEAA went on to explain the reliance of journalists on confidential sources and their concern that the Bill threatens the confidentiality of those sources:

> Journalists rely on sources of information to carry out these duties. At times, those sources request anonymity – perhaps because they are in fear or could be subject to some form of violence, harassment or intimidation, particularly if they are a 'whistleblower'.
>
> The Bill threatens to expose the identity of sources and journalists as well as the communications between them and information they exchange.
>
> The Bill will undoubtedly undermine the crucial ethical obligation of journalists to protect the identity and information of confidential sources.
>
> This erosion of journalist privilege that is the consequence of the Bill will have a chilling effect on whistleblowers seeking to expose illegality, corruption or wrongdoing.[143]

6.203 The MEAA noted that the majority of legal jurisdictions, including the Commonwealth, recognise the principle of journalist privilege, and recommended that the Bill not proceed, but if it does:

> that appropriate checks and balances be introduced to ensure that the national security laws cannot be used to impede, threaten, contain or curtail legitimate reporting of matters in the public interest and that journalists and their confidential sources are free to continue to interact and communicate without being subjected to surveillance that would undermine the principles of press freedom.[144]

142 Media, Entertainment and Arts Alliance, *Submission 90*, p. 3.

143 Media, Entertainment and Arts Alliance, *Submission 90*, p. 3.

144 Media, Entertainment and Arts Alliance, *Submission 90*, pp. 9-10.

6.204 In response to suggestions that special status be afforded to the telecommunications data of journalists, the Attorney-General's Department noted the importance for the powers to apply generally and that legitimate whistleblowers would be protected by public interest disclosure legislation:

> Disclosures of data are available to support the enforcement of the criminal law, administration of pecuniary penalties and the protection of the public revenue. It is not appropriate to afford a special status to particular types of communications as powers of this type should, by their nature, be applied generally. However, to the extent that concerns relate to the disclosure of the identity of legitimate whistle-blowers, it is important to note that such persons have specific protection under the *Public Interest Disclosures Act 2013* (PID Act). The effect of those protections is that disclosures by legitimate whistle-blowers are not criminal acts. Accordingly, telecommunications data would not be available by reason of the disclosure.[145]

6.205 A submission by joint media organisations noted a recent report by Human Rights Watch in respect of the United States that large-scale surveillance makes it difficult for journalists to communicate with sources securely. The submission noted:

> The cumulative impact of these matters is a chilling effect on news gathering through increasing the perceived risks to sources including whistleblowers – in an environment which has also heightened the risk to news gathering by criminalising some reportage and not providing adequate protections for some categories of whistleblowers.[146]

6.206 Private Media raised similar concerns in its submission, noting the importance of the media as a watchdog, and the critical importance of protecting confidential sources:

> Whistleblowers and confidential sources are fundamental to this media role. Without individuals who are prepared to reveal wrongdoing and provide transparency, the media is unable to perform this role and powerful interests can operate with less accountability. For such individuals, anonymity and confidentiality are crucial … It is thus critical that the media is able to offer confidential sources protection – and this is already

145 Attorney-General's Department, *Submission 27*, pp. 21-22.

146 Joint media organisations, *Submission 125*, p. 3.

> recognised in federal legislation such as the Evidence Amendment (Journalists Privilege) Act 2010.
>
> However, a data retention scheme of the kind proposed in the Bill will make it significantly easier for powerful interests -- whether governments, well-resourced individuals or corporations – to pursue, harass, prosecute and intimidate whistleblowers who contact media outlets, because information relating to who has contacted journalists via any form of electronic communication will be stored for two years …[147]

6.207 Private Media referred in its submission to upcoming changes in the United Kingdom, and suggested similar arrangements should be introduced in Australia:

> The UK government, which last year introduced its own version of data retention, has acknowledged that police misuse of powers to access metadata had been 'entirely inappropriate' and will change the UK's data access laws to require police to obtain a warrant if they want to obtain a journalists' metadata, with a presumption that access would not be granted if the journalist was acting in the public interest.[148]

6.208 On this issue the Attorney-General's Department provided the following evidence in their submission:

> On 9 December 2014, the UK Home Office published a draft Code of Practice discussion paper on access to data. This issue of access to journalists' telecommunication during the investigation of crimes had been raised as an issue by that profession. The draft code of practice makes clear that communications data is not subject to any form of professional privilege. However, the Code notes that access to data relating to some professions may have a higher degree of privacy interference (the draft code specifies doctors, lawyers, journalists, MPs and ministers of religion).
>
> Some media reports had suggested that the UK Government was considering requiring law enforcement agencies to obtain warrants to access journalists' data. Rather than warrants, the Home Office proposes that authorising officers should give special consideration to necessity and proportionality when considering authorising the disclosure of data relating to the particular professions noted above.[149]

147 Private Media, *Submission 77*, p. 2.

148 Private Media, *Submission 77*, p. 2.

149 Attorney-General's Department, *Submission 27*, p. 22.

6.209 The supplementary submission from joint media organisations emphasised the concern of those organisations that the collection and storage of metadata could be accessed to identify journalists' sources, making it less likely that sources will share information and consequently have a chilling effect on reporting in the public interest. The submission proposed a tiered range of amendments to address this concern which can be summarised (in descending order of preference) as follows:

- media exemption from all three tranches of national security legislation;
- media exemption for the Bill;
- requirement for a warrant to access metadata of journalists and their sources;
- persons empowered to authorise requests to access data must be limited to the most senior officials of an agency, and the threshold for access must be more objective.[150]

Committee comment

6.210 The Committee recognises that certain telecommunications data has the potential to possess an additional level of sensitivity because of the nature of the relationship of those communicating, including client legal privilege that applies to certain communications between lawyers and their clients, and journalist relationships with confidential sources.

6.211 In the context of client legal privilege the Committee notes the evidence from the Attorney-General's Department that privilege attaches to the content of the communications, and that access to telecommunications data will not include any such content.

6.212 The Committee acknowledges the evidence from the Law Council of Australia that telecommunications data can nonetheless reveal a range of information about the communications between a lawyer and client from which certain inferences may be able to be made.

6.213 However, the Committee does not consider, on the evidence available, that there is a need for additional legislative protection in respect of accessing telecommunications data that may relate to a lawyer.

6.214 In the context of journalists and their sources, the Committee notes the capacity for telecommunications data to be used to identify confidential sources. The Committee acknowledges the claims that this may have a 'chilling impact', although the Committee also notes that in some circumstances, such as the investigation of serious crimes, it may be

150 Joint media organisations, *Submission 125.1*, pp. 1-3.

appropriate and proper for journalists to be investigated by law enforcement agencies.

6.215 The Committee acknowledges the importance of recognising the principle of press freedom and the protection of journalists' sources. The Committee considers this matter requires further consideration before a final recommendation can be made.

6.216 In the absence of pre-access oversight by an independent body, the Committee also considers it reasonable to require the Ombudsman or Inspector-General of Intelligence and Security (IGIS), as appropriate, to be notified of the making of an authorisation which is for the purpose of determining the identity of a journalist's sources.

Recommendation 26

The Committee acknowledges the importance of recognising the principle of press freedom and the protection of journalists' sources. The Committee considers this matter requires further consideration before a final recommendation can be made.

The Committee therefore recommends that the question of how to deal with the authorisation of a disclosure or use of telecommunications data for the purpose of determining the identity of a journalist's source be the subject of a separate review by this Committee.

The Committee would report back to Parliament within three months.

In undertaking this inquiry, the Committee intends to conduct consultations with media representatives, law enforcement and security agencies and the Independent National Security Legislation Monitor. The review will also consider international best practice, including data retention regulation in the United Kingdom.

Recommendation 27

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to require agencies to provide a copy to the Commonwealth Ombudsman (or Inspector General of Intelligence and Security (IGIS) in the case of ASIO) of each authorisation that authorises disclosure of information or documents under Chapter 4 of the Act for the purpose of determining the identity of a journalist's sources.

The Committee further recommends that the IGIS or Commonwealth Ombudsman be required to notify this Committee of each instance in which such an authorisation is made in relation to ASIO and the AFP as soon as practicable after receiving advice of the authorisation and be required to brief the Committee accordingly.

Destruction of accessed telecommunications data

6.217 The TIA Act does not currently contain any requirements in in respect of destruction of telecommunications data accessed by enforcement agencies or ASIO. The Law Council of Australia identified in its submission this lack of destruction requirements in respect of accessed data, and supported the inclusion of such a requirement:

> Chapter 4 of the TIA Act does not require enforcement agencies to destroy in a timely manner telecommunications data containing personal information which is irrelevant to the agency or no longer needed.
>
> The Law Council strongly supports the inclusion of provisions which establish positive obligations of this kind.[151]

6.218 The Law Institute of Victoria similarly queried what requirements will be put in place to ensure the timely destruction of retained data by agencies after the purpose for which the data was requested has been satisfied.[152]

6.219 At a public hearing, the IGIS noted the lack of a legislative requirement for ASIO to delete telecommunications data that is no longer needed:

> My second point is about what happens to data once it has been lawfully obtained by ASIO. This is an issue that is actually broader than telecommunications data, but it is highlighted by the increase in the volume of data that would be available under the proposed scheme. There are certainly good reasons ASIO may need to keep

151 Law Council of Australia, *Submission 126*, p. 25.

152 Law Institute of Victoria, *Submission 117*, p. 5.

> some data for a long time. But there is other data that, although it is obtained lawfully, turns out not to be relevant to security or is no longer relevant to security after a period of time. The balance between security and privacy, in my view, requires that this information should not be retained indefinitely, and I think that the general public would expect that material found not to be relevant to security would be deleted after a period of time.
>
> There are currently provisions that allow for the destruction of data by ASIO, but at the moment there seems to be little or no legislative requirement for ASIO to delete telecommunications data or other material that is no longer needed. In 2010 my predecessor looked at the retention of data by ASIO and suggested that ASIO should modify its policies and practices. The agreement between ASIO and the National Archives of Australia was reviewed in 2012, and the subject of the retention and destruction of data by ASIO is a focus for my office this year. While this project is ongoing, I do think this matter could also usefully be examined as part of the review of the Attorney-General's guidelines previously proposed by this committee and agreed to by government.[153]

6.220 When asked by the Committee whether there should be a compulsion for the agency, when it is finished with the data and it is not of any use in terms of legal purposes, to destroy the data, the IGIS stated:

> I can understand that there would be an impost in terms of resources to assess that at a certain point in time. However, I think that needs to be balanced against what I would consider to be the general public expectation that, if matter is found to be not relevant to security or no longer relevant to security, it should be deleted. I am not sure that balance is correct at the moment.[154]

6.221 The IGIS was also asked by the Committee to comment on whether there could be elements of the information that ASIO holds, such as pattern of life analysis, that they retain to see where investigations might take those patterns into the future. Dr Thom stated:

---

153 Dr Vivienne Thom, Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 29 January 2015, p. 37.

154 Dr Vivienne Thom, Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 29 January 2015, p. 40.

> Absolutely. There is a large amount of information that would have to be retained forever according to the guidelines, and I have no concerns about that at all.[155]

6.222 In response to a question on this issue from the Committee on whether the Bill should contain a mandatory destruction component, Professor George Williams gave his opinion that such a regime would be appropriate:

> I think that would allay community concerns that their private information may be sought, perhaps legitimately, but then held for an extremely long period of time—well past the nature of the investigation—and perhaps looked at again sometime down the track in less appropriate circumstances. I think the community concern about what some see as a blanket surveillance regime is that the onus is on parliament to make sure a scheme is designed that is very well tailored to the problem. And there is a problem that needs to be met here. We need a bill that removes many of the quite significant loose ends, that being one of them, that as yet have not been adequately dealt with.[156]

Committee comment

6.223 The Committee acknowledges the importance of ensuring that agencies are subject to appropriate obligations in respect of the retention and destruction of telecommunications data. In this respect the Committee notes the application of the various federal and state privacy and archives obligations, as well as agency specific legislation.

6.224 The Committee considers it has not received sufficient evidence to form a conclusion as to whether there is a need for a discrete obligation for destruction of telecommunications data to be inserted into the TIA Act, and if so, what form that requirement should take.

6.225 In respect of ASIO, the Committee notes that the agreement between ASIO and the National Archives was reviewed in 2012 and notes that the retention and destruction of data by ASIO is to be a focus for the IGIS this year. The Committee welcomes these ongoing discussions between the IGIS and ASIO in respect of destruction of information, and the planned review of the Attorney-General's Guidelines later this year.

---

155 Dr Vivienne Thom, Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 29 January 2015, p. 40.

156 Professor George Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 7.

Recommendation 28

The Committee recommends that the Attorney-General's Department oversee a review of the adequacy of the existing destruction requirements that apply to documents or information disclosed pursuant to an authorisation made under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* and held by enforcement agencies and ASIO.

The Committee further recommends that the Attorney-General report to Parliament on the findings of the review by 1 July 2017.