2

Telecommunications Interception

2.1 In its discussion paper, the Attorney-General's Department (AGD) notes that the current *Telecommunications (Interception and Access) Act 1979* (TIA Act):

> ...reflects the use of telecommunications and the structure of the telecommunications industry that existed in 1979 when the Act was made. Many of these assumptions no longer apply, creating significant challenges for agencies in using and maintaining their investigative capabilities under the Act.[1]

2.2 Therefore, the Australian Government has proposed a series of reforms to the telecommunications interception regime that are designed better reflect the 'contemporary communications environment'.[2]

2.3 In particular, the AGD identified four aspects of the legislation as requiring reform:

- Strengthening the safeguards and privacy protections in line with contemporary community expectations;
- Reforming the lawful access regime for agencies;
- Streamlining and reducing complexity; and
- Modernising the cost sharing framework.[3]

2.4 This chapter will examine each of those proposals. Before doing so, the Committee notes the evidence from interception agencies and the AGD that these

---

1 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 12.

2 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 12.

3 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 22.

proposals should be considered in the context of a holistic revision of the TIA Act:

> The magnitude of current and anticipated change to the telecommunications landscape means it is now timely to consider whether the privacy needs of Australians and the investigative needs of law enforcement and national security agencies are best served through continuous ad-hoc change or whether the time is right to put in place a new interception framework that squarely focuses on the contemporary communications environment. The Department considers that holistic reform would establish a new foundation for the interception regime that enables users and participants, as well as the broader Australian community to understand their powers, rights and obligations.[4]

2.5 The Committee's view on whether a new interception regime is necessary will be provided following the consideration of the individual proposals for reform of the TIA Act.

Strengthening the safeguards and privacy protections

2.6 The AGD discussion paper expresses a desire to examine the 'safeguards and privacy protections under the lawful access to communications regime' in the TIA Act. In particular, the discussion paper seeks to examine:

- The legislation's privacy protection objective;
- The proportionality tests for issuing warrants;
- Mandatory record-keeping standards; and
- Oversight arrangements by Commonwealth and State Ombudsmen.[5]

The legislation's privacy protection objective

2.7 As the discussion paper notes, the interception of telecommunications is 'a powerful and cost effective tool' for law enforcement and intelligence agencies. However, the discussion paper also notes that the ability to intercept telecommunications data and content must be balanced with the protection of privacy:

> The primary objective of the current legislation governing access to communications is to protect the privacy of users of telecommunications

4 Attorney-General's Department, *Submission No. 218*, pp. 2-3

5 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, pp. 7-8.

> services in Australia by prohibiting covert access to communications except as authorised in the circumstances set out in the TIA Act.[6]

2.8 The discussion paper proposes that the safeguards and privacy protections of the interception regime be strengthened 'in line with contemporary community expectations'.

2.9 Many of the submissions and much of the testimony provided to the Committee focused upon the privacy impact of proposals for reform of the TIA Act, with submitters and witnesses noting that one of the primary objectives of the telecommunications interception regime is to protect the privacy of people against the intrusion of interception.

2.10 The proposal for a privacy objective drew broad support, from privacy advocates, private submitters, law enforcement and investigative agencies alike. The Western Australian Police stated:

> It is recognised that the privacy protection objective is a fundamental principle which underlies the TIA Act. It is important to protect the privacy of users of telecommunications services by prohibiting covert access to communications except as authorised by the TIA Act.
>
> …
>
> The introduction of a privacy focus objective clause into the TIA Act is appropriate, and would ensure that privacy protection is a consideration in the interpretation and application of the law.[7]

2.11 The Law Council of Australia expressed strong support for the introduction of a privacy focused objects clause, and made several suggestions of possible provisions on which it could be modelled:

> Such a clause could be modelled on Article 17 of the International Covenant on Civil and Political Rights (ICCPR) which provides that:
>
> - 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'
>
> Article 8 of the European Convention on Human Rights (ECHR) also provides a possible model for such an objects clause. It provides that:
>
> - 'Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being

6 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 12.

7 Western Australia Police, *Submission No. 203*, p. 6.

> of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'[8]

2.12 The NSW Council for Civil Liberties indicated that a privacy objective would provide an interpretive aid to issuing authorities when considering warrant applications:

> A privacy objective should be introduced into the legislation, as the Government proposes. It should be made clear that the privacy objective limits the operations of government agencies as well as those of other persons. This will assist judicial authorities to be tougher in their scrutiny of warrant applications. [9]

2.13 The AGD discussion paper refers to strengthening privacy protections in line with contemporary community expectations, but provides no detail on what those expectations are. On that point, Privacy Victoria submitted:

> …it is important that we consider what 'contemporary community expectations' regarding privacy actually are. For example, in 2007 the Office of the Privacy Commissioner commissioned a survey into community attitudes to privacy. This survey was undertaken at the cusp of the social media boom. In the survey, 86% of respondents felt that it was a serious breach of privacy where a government department monitors an individual's activities on the internet, recording information on sites visited without the individual's knowledge. Similarly, 50% were more concerned than two years previous (2005) about providing information over the internet. I consider that these numbers would be greater today, given the mass of information collected by electronic means.[10]

2.14 The Information Commissioner suggested that the *Privacy Act 1988* reflects community privacy expectations:

> The OAIC considers that the *Privacy Act 1988* (C'th) (Privacy Act), as the privacy oversight instrument the public is most familiar with, reflects existing community expectations. Accordingly, incorporating the core principles and values that underpin the Privacy Act into the other privacy accountability frameworks will help ensure that they remain consistent with community values and expectations.[11]

---

8 Law Council of Australia, *Submission No. 96*, pp. 21-2.

9 NSW Council for Civil Liberties, *Submission No. 175*, p. 15.

10 Privacy Victoria, *Submission No. 109*, p. 3.

11 Office of the Australian Information Commissioner, *Submission No. 183*, pp. 1-2.

2.15 While supportive of a privacy objective, the Western Australian Corruption and Crime Commission noted the need to balance privacy with investigative needs:

> The Commission supports the primary objective of the TIA Act which seeks to protect the privacy of individuals who use the Australian telecommunications system. The TIA Act does this by making it an offence to intercept communications passing over the telecommunications system. However this needs to be balanced against Australia's law enforcement and national security interests.[12]

2.16 Similarly, Privacy Victoria assisted the Committee by noting the need to balance other considerations:

> Privacy is not an absolute right. A balance must be struck between privacy and other rights, including the public interest in protecting the safety and security of Australians. This balancing act is a central tenet to privacy legislation around the world, and at times privacy must give way to other public and private interests.[13]

2.17 The Committee recognises the dual objectives of the TIA Act: to protect the privacy of communications by prohibiting unlawful interception, while enabling limited interception access for the investigation of serious crime and threats to national security. Express recognition of these objectives within the legislation would provide clarity of the purposes of the legislation and some interpretive guidance.

12 Western Australian Corruption and Crime Commission, *Submission No. 156*, p. 4.

13 Privacy Victoria, *Submission No. 109*, p. 1.

Recommendation 1

The Committee recommends the inclusion of an objectives clause within the *Telecommunications (Interception and Access) Act 1979*, which:

- **expresses the dual objectives of the legislation –**
  - ⇒ **to protect the privacy of communications;**
  - ⇒ **to enable interception and access to communications in order to investigate serious crime and threats to national security; and**
- **accords with the privacy principles contained in the *Privacy Act 1988*.**

The proportionality tests for issuing warrants

2.18 The AGD submission outlined the factors which must be considered by an issuing authority prior to issuing telecommunications interception warrants:

> The independent authority may issue the warrant if satisfied from the facts outlined in the affidavit that:
> - there are reasonable grounds for suspecting that the person is using or is likely to use the service;
> - that information obtained under interception would be likely to assist the investigation of a serious offence in which the person is involved;
> - and having regard to:
>   - ⇒ the privacy of any persons likely to be interfered with by interception;
>   - ⇒ the gravity of the conduct being investigated; and
>   - ⇒ the extent to which other methods of investigating the offence have been exhausted or would prejudice the investigation.[14]

2.19 Submitters expressed support for the existence of the proportionality tests within the TIA Act, but expressed frustration about the absence of detailed proposals on which to comment. For example, Mr Bernard Keane stated:

14 Attorney-General's Department, *Submission No. 218*, Attachment A p. 1.

> The paper is unclear about exactly what 'strengthening' is intended beyond a review and consideration of 'a privacy focused objects clause'. Strengthening privacy laws and reviewing checks and balances is of course unobjectionable; but AGD has failed to even clearly describe its thinking on this important issue.[15]

2.20 The Law Council of Australia noted that one way to strengthen the privacy protections within the TIA Act is to ensure consistent consideration of the impact of privacy before any power under the TIA Act is exercised:

> …the requirement to consider the extent to which the exercise of a power will interfere with personal privacy currently applies to the issuing of certain TIA Act warrants, but not all.
>
> For this reason, the Law Council supports the inclusion of a single, consistent privacy test in all warrant applications and in all authorisations to intercept, access or disclose telecommunications or telecommunications data.[16]

2.21 The Australian Federal Police (AFP) expressed support for strengthening the proportionality test for telecommunications interception warrants, noting that the current formulation has 'becoming increasingly out of balance to the changes in the way people communicate, the technology available to communicate and the use of that technology to commit crime'.[17] As a result, the AFP:

> …sees benefit in strengthening the existing proportionality test to include consideration of the overall community good served by the investigation for which the interception is sought.[18]

2.22 The Western Australia Police submitted that 'the current provisions of the TIA Act provide sufficient scope for the proportionality test to be properly applied'[19] and did not seek change to the proportionality test.

2.23 The Committee notes the useful discussion of proportionality tests provided by the Human Rights Law Centre in its submission:[20]

---

15 Mr Bernard Keane, *Submission No. 117*, p. 3. See also Mr Robert Batten, *Submission No. 50*, p. 3; Mr Ian Quick, *Submission No. 95*, p. 4.

16 Law Council of Australia, *Submission No. 96*, p. 23.

17 Australian Federal Police, *Submission No. 163*, p. 8.

18 Australian Federal Police, *Submission No. 163*, p. 8.

19 Western Australia Police, *Submission No. 203*, p. 6. See also: Western Australian Corruption and Crime Commission, *Submission No. 156*, pp. 4-5.

20 Human Rights Law Centre, *Submission No. 140*, pp. 2-3.

> Put broadly, general provisions setting out a proportionality analysis require that any limitation of rights be reasonable and demonstrably justified in a free and democratic society.

2.24 The Committee considers the TIA Act must continue to require the consideration of proportionality in authorising the use of telecommunications interception as an intrusive investigative technique. Given the evidence cited above the Committee believes it is appropriate that a review of the TIA Act's proportionality tests be carried out. Any review of the proportionality tests must consider a range of matters to be included in the test, including the gravity of the conduct being investigated, the privacy intrusion of proposed investigative activity, the public interest served by the proposed investigative activity, and whether other less privacy intrusive investigative techniques would be effective.

2.25 The Committee further considers there would be merit when reviewing the proportionality tests to examine the application of those tests across the range of powers in the TIA Act (interception, access to stored communications, and access to telecommunications data).

Recommendation 2

The Committee recommends the Attorney-General's Department undertake an examination of the proportionality tests within the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Factors to be considered in the proportionality tests include the:

- **privacy impacts of proposed investigative activity;**
- **public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and**
- **availability and effectiveness of less privacy intrusive investigative techniques.**

The Committee further recommends that the examination of the proportionality tests also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers in the TIA Act.

Mandatory record-keeping standards

2.26 The AGD discussion paper outlines the current TIA Act record-keeping requirements:

> Record keeping and accountability obligations require law enforcement agencies to keep records relating to documents associated with the

> warrants issued and particulars relating to warrant applications (such as whether an application was granted or refused) and each time lawfully intercepted information is used, disclosed, communicated, entered into evidence or destroyed. Agency heads must also report to the Attorney-General on the use and communication of intercepted information within three months of a warrant ceasing to be in effect. The Attorney-General's Department must prepare an annual statistical report about the use of powers under the TIA Act, which the Attorney-General tables in Parliament.[21]

2.27 The AGD discussion paper goes on to argue 'the current regime is focused on administrative content rather than recording the information needed to ensure that a particular agency's use of intrusive powers is proportional to the outcomes sought'.[22] The AGD therefore recommends:

> Consideration should be given to introducing new reporting requirements that are less process oriented and more attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes.[23]

2.28 Two submissions suggested that a streamlined reporting regime could lead to significant weakening of oversight. For example, Mr Bernard Keane stated:

> An alternative view is that 'inflexible' and 'one size fits all' provisions ensure that agencies cannot try to avoid reporting obligations and report in a manner that will enable meaningful comparisons over time and with other agencies. For relatively minor regulatory requirements, a 'co-regulatory approach' such as that proposed by AGD might be appropriate, but given the serious nature of the issues on which law enforcement and intelligence agencies are being asked to report, it is wholly inappropriate to leave it up to agencies themselves to determine exactly how and what they report within a general remit. This would represent a significant weakening of accountability in an area where there is already too little scrutiny.[24]

2.29 The Committee received evidence from law enforcement agencies regarding the application of the existing record-keeping requirements. For example, the AFP stated:

---

21 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 26.

22 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 26.

23 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 26.

24 Mr Bernard Keane, *Submission No. 117*, p. 3. See also Electronic Frontiers Australia, *Submission No. 121*, pp. 12-13

> The AFP believes the current legislated scheme needs review. It may have reached the point where it is too focussed on administrative requirements, rather than providing the basis for Parliament and the Ombudsman to ensure agencies are using the powers in the Act in a way that is consistent with the principles underlying the Act. There would be value in redrafting the legislation to include simplified, comprehensible and meaningful accountabilities and annual reporting obligations to enhance community understanding of the regime and its safeguards.[25]

2.30 In support of this observation, the AFP cited the example of the requirement to provide a certified copy of each warrant despite the obvious efficiencies provided by email or facsimile communications.[26]

2.31 Similarly, the Western Australia Corruption and Crime Commission submitted:

> The Commission fully supports a robust regime of mandatory record-keeping standards for agencies exercising powers under the TIA Act. The Commission acknowledges that effective oversight of agencies' use of these powers requires appropriate record-keeping standards sufficient to show compliance with the legislation. However it is the view of the Commission that many of the requirements of the current Act create unnecessary duplication of records and the creation of further records which no longer serve the original purpose of ensuring compliance with the Act and the creation of a robust compliance regime.[27]

2.32 The Law Council of Australia expressed support for streamlining the record-keeping requirements of the TIA Act to ensure they provided effective accountability:

> The Law Council strongly supports efforts to ensure that the reporting requirements and oversight mechanisms contained in the TIA Act are '…attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes', as suggested by the Discussion Paper. This may involve review and reform of the different procedural and administrative requirements currently contained in the TIA Act relating to reporting, and to the role of the Commonwealth Ombudsman and his or her State and Territory counterparts. It may also involve consideration of additional or alternative mechanisms to enhance accountability under the TIA Act.[28]

---

25 Australian Federal Police, *Submission No. 163*, p. 9.

26 Australian Federal Police, *Submission No. 163*, p. 9.

27 Western Australia Corruption and Crime Commission, *Submission No. 156*, p. 5. See also Western Australia Police, *Submission No. 203*, pp. 6-7.

28 Law Council of Australia, *Submission No. 96*, p. 48.

2.33 The Law Council of Australia cautioned against 'removing requirements for agencies to collect and record certain information about the exercise of their powers under the Act' citing the example of the register of warrants maintained by the Secretary of the AGD.[29]

2.34 The Committee strongly supports the need for record-keeping requirements as a means of ensuring meaningful oversight and accountability. The TIA Act enables law enforcement and security agencies to exercise intrusive powers. It is vital to the ongoing ability of those agencies to use those powers to be able to demonstrate adherence to the accountability requirements of the TIA Act. During the inquiry, the Committee received assurance from the Commonwealth Ombudsman's office and the Inspector-General of Intelligence and Security of the high level of accountability discharged by the interception agencies.[30]

2.35 The Committee acknowledges, however, that record-keeping is not an end in itself, and must be designed to provide substantive rather than administrative accountability. The Committee is satisfied that there is scope for achieving efficiencies by reviewing the existing reporting requirements without undermining accountability. Further, the Committee considers there is scope to enhance accountability by removing otiose reporting requirements.

Recommendation 3

The Committee recommends that the Attorney-General's Department examine the *Telecommunications (Interception and Access) Act 1979* with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought.

Oversight arrangements by the Commonwealth and State Ombudsmen

2.36 The AGD discussion paper outlines the present oversight arrangements for law enforcement agencies:

> Oversight of law enforcement agencies' use of powers is split between the Commonwealth Ombudsman and equivalent State bodies in relation to interception activities. The Commonwealth Ombudsman inspects the records of both Commonwealth and State agencies in relation to stored communications. This split in responsibility contrasts with the

29 Law Council of Australia, *Submission No. 96*, p. 48.

30 See for example, Inspector-General of Intelligence and Security, *Submission No. 185*, p. 8.

> *Surveillance Devices Act 2004*, where the Commonwealth Ombudsman inspects all agencies.[31]

2.37 The AGD goes on to note that the prescriptive form of the TIA Act oversight provisions 'impede the Ombudsman's ability to report on possible contraventions and compliance issues by prescribing detailed and time limited procedures that need to be checked for administrative compliance, rather than giving the Ombudsman scope to determine better ways of assisting agencies to meet their requirements.'[32]

2.38 The Committee received submissions from law enforcement agencies expressing support for the review of the oversight arrangements to clarify the roles played by different oversight bodies. For example, the Western Australia Police stated:

> The TIA Act currently creates a system based on dual oversight by both Commonwealth and State Ombudsman. The role of the oversight body, and the scope of inspection, could be better defined within the TIA Act.
>
> For WA Police, stored communications are inspected by the Commonwealth Ombudsman, annually. Inspections of all other TI Warrants, and the corresponding revocations, destruction of, and associated record keeping, is conducted by the State Ombudsman, on a regular basis.
>
> On occasion, the Commonwealth Ombudsman has made comment on the content of an affidavit in support of an application for a stored communications warrant, and has questioned the appropriateness of the application. WA Police is of the opinion that the determination of the application, and the appropriateness or otherwise of the information contained in the affidavit is a matter for the issuing authority, not the oversight body. It is noted that the issuing authority has the power to receive information in both written and oral form.
>
> An examination of the existing oversight arrangements, the clarity of the role, and the practicality of a single oversight body is supported by WA Police.[33]

2.39 Similarly, Telstra noted a desire for consistency of oversight arrangements:

> Telstra agrees that there must be consistent and practical arrangements put in place to enable oversight by both Commonwealth and State Ombudsmen aimed at strengthening the safeguards and privacy

---

31 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 26.

32 Attorney-General's Department, Equipping Australia against emerging and evolving threats, Discussion Paper, July 2012, p. 26.

33 Western Australia Police, *Submission No. 203*, p. 7.

> protections under the TIA Act and the Telco Act to ensure the security and privacy of customer communications.[34]

2.40 The Office of the Australian Information Commissioner noted risks inherent in the fragmentation of oversight arrangements:

> …the OAIC notes that the fragmentation of existing oversight arrangements can make it difficult for the public to discern which oversight body is responsible for overseeing the access and interception activities of a particular law enforcement agency. The OAIC is mindful that the nature of the activities undertaken by law enforcement agencies may mean that, in certain circumstances, it is not appropriate for these activities to be made public. In these circumstances, it is particularly important that effective oversight arrangements exist to ensure that these agencies are not exceeding their lawful authority and to give the public confidence that their personal information is being handled in accordance with contemporary community expectations. The OAIC suggests that providing the public with clear information about which oversight bodies are responsible for overseeing the access and interception activities of specific law enforcement agencies would provide a more appropriate level of transparency.[35]

2.41 The Law Council of Australia noted its support for consideration of a model similar to the *Surveillance Devices Act 2004* (Cth) whereby the Commonwealth Ombudsman would be the sole oversight body for law enforcement agencies under the TIA Act:

> The Law Council supports consideration of this model for potential application to the TIA Act warrant regime, which currently imposes inspection and reporting obligations on State bodies in respect of State agencies' interception activities under the TIA Act. However, if a reform of this nature is to be pursued it must be developed in consultation with State and Territory Ministers and should not detract from the other reporting requirements outlined in the TIA Act…[36]

2.42 The Committee believes that reviewing the TIA Act oversight regime to ensure the application of consistent standards of accountability and a single perspective on best practice is warranted. On the evidence before it, the Committee was not persuaded that the Surveillance Devices Act model is appropriate. The Committee is also aware of significant jurisdictional issues inherent in progressing this matter..

---

34 Telstra, *Submission No. 189*, p. 6.

35 Office of the Australian Information Commissioner, *Submission No. 183*, p. 12.

36 Law Council of Australia, *Submission No. 96*, p. 50.

Recommendation 4

The Committee recommends that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the *Telecommunications (Interception and Access) Act 1979*.

Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism.

The Committee also recommends the Attorney-General's Department consult with State and Territory ministers prior to progressing any proposed reforms to ensure jurisdictional considerations are addressed.

Reforming the lawful access regime for agencies

2.43 The second aspect of the legislation in need of reform identified by the AGD discussion paper is the current lawful access regime. The AGD identifies several areas for specific examination. First, it seeks to reform the lawful access to communications regime contained in the TIA Act by 'reducing the number of agencies eligible to access communications information'. Second, it seeks to standardise warrant tests and thresholds. Third, it seeks to expand 'the basis of interception activities'.[37]

Reducing the number of agencies eligible to access communications information

2.44 The AGD discussion paper states that a reduction in the number of agencies able to access communications information is contemplated 'on the basis that only agencies that have a demonstrated need to access that type of information should be eligible to do so.'[38]

2.45 A range of submissions cited with approval the proposal to reduce the number of agencies able to access communications information, but noted the difficulty in identifying which agencies should have these powers removed. Ms Stella Gray commented:

37 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, pp. 8, 9.

38 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 24.

> Reducing the number of government agencies which have access to individuals' private communications, reduces the ability to abuse the TIA. However, there is insufficient detail here on which agencies are being considered for reduction in such powers.[39]

2.46 Similarly, Liberty Victoria submitted:

> Liberty Victoria agrees that lawful access by agencies to telecommunications data ought to be restricted to protect the privacy rights of individuals. Liberty Victoria agrees that reducing the number of agencies able to access sensitive data is, in principle, important and necessary. Liberty Victoria would, however, like to understand further how the Government proposes to determine which agencies are able to access this data, to ensure that there are real and substantive security benefits proportionate to the greater privacy risks that arise when information is more widely disseminated.
>
> The Discussion Paper's suggestion that agencies must have a 'demonstrated need' to access information, while a good suggestion (indeed, a suggestion that one would have hoped already applied to agencies' access to personal information), is too general to offer a detailed response. For example, it does not indicate how 'need' would be demonstrated as opposed to 'operational convenience'..[40]

2.47 The Attorney-General's Department outlined to the Committee which agencies have access to telecommunications information:

> Currently, access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits an 'enforcement agency' to authorise a C/CSP 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 for national security purposes.
>
> An enforcement agency is broadly defined as all interception agencies as well as a body whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue. In practice, the range of agencies that are enforcement agencies and which authorise the disclosure of telecommunications data is very broad and includes Shire Councils, Government Departments and Agencies such as Centrelink and bodies as the Royal Society for the

39 Ms Stella Gray, *Submission No. 152*, p. 7.

40 Liberty Victoria, *Submission No. 143*, p. 6. See also Mr Bernard Keane, *Submission No. 117*, pp. 3-4; Senator Scott Ludlam, *Submission No. 146*, p. 3; Mr Ian Quick, *Submission No. 95*, p. 5.

> Prevention of Cruelty to Animals (RSPCA) (which plays a role in investigating assaults and other criminal acts against animals).[41]

2.48 The Committee noted that in 2010-11 there were 251,631 requests for access to telecommunications data from a variety of agencies including police forces, anti-corruption bodies, Commonwealth and State and territory departments, local shire councils, animal protection authorities, roads authorities, revenue offices, and child support agencies.[42]

2.49 Ms Irene Graham submitted that the range of agencies able to access stored communications and communications data should be reduced:

> The range of agencies should certainly be reduced, and probably most especially by deleting all, or most, of the civil and pecuniary penalty agencies that acquired power to obtain access to stored communications when the 'stored communications' warrants were introduced in 2006 (although such agencies were not and still are not authorised to obtain interception warrants).
>
> …
>
> There absolutely does need to be a competent review conducted into which of such agencies have a clearly demonstrated need to access stored communications and/or telecommunications 'data' in specific circumstances, together with consideration of the type of offences and the penalties that apply to any offences in relation to which such agencies claim 'a need'.[43]

2.50 Telstra submitted the TIA Act could be amended to differentiate between types of telecommunications data, with limited agencies being permitted to access sets of data considered to be more sensitive:

> Telstra believes there is some merit in adopting a two-tiered communications data access regime to address potential risks of allowing access to customer data for the investigation of lesser offences. Under this type of regime, data readily available through C/CSP customer information systems could be provided under the current threshold test and would potentially remain accessible to a larger number of enforcement agencies and LENSAs [Law Enforcement and National Security Agencies].
>
> Under this construct, access to more intrusive communications data, e.g. URLs, IP addresses or 'created' tailored data sets proposed under the data

41 Attorney-General's Department, *Submission No. 218*, p. 9.

42 Telecommunications (Interception and Access) Act 1979 Annual Report 2010-11, pp. 62-5.

43 Ms Irene Graham, *Submission No. 135*, p. 5.

> retention regime, would only be provided to a limited number of LENSAs and would require higher approval thresholds to be satisfied.[44]

2.51 An alternative approach was submitted by the Australian Mobile Telecommunications Association and Communications Alliance in their joint submission:

> The Associations believe that rather than looking to define the number of agencies that are eligible to access communications information (that being content and transactional data), a preferred approach should be to reserve access to communications information solely for purposes of addressing instances of serious crime or threats to national security. The nature of the crime/threat in each instance would then determine the type of information required, and the agency/agencies who are eligible to obtain access. If this approach is taken it will be important to be clear about what constitutes 'serious crime'.[45]

2.52 The Committee was not able within the confines of this inquiry to examine the justification for each enforcement agency to be able to continue to access telecommunications data. It was clear from the evidence however that the present definition of enforcement agency, being broad and inexhaustive, leaves the potential for many agencies to request access to telecommunications data without independent scrutiny other than from the telecommunications providers who receive those requests. This is not an acceptable burden to place on telecommunications providers, nor is the Committee convinced that this is an effective accountability mechanism.

2.53 The Committee considers the appropriate mechanism to justify access to telecommunications data is the threshold at which access is granted. The threshold acts to establish the level of gravity of the conduct which must be under investigation before the privacy intrusion of accessing telecommunications data can be justified.

2.54 The Committee is satisfied that access to telecommunications data for serious crime and threats to security is justified. Access for agencies not enforcing the criminal law or investigating security threats should be subject to further review.

---

44 Telstra, *Submission No. 189*, p. 6.

45 Australian Mobile Telecommunications Association – Communications Alliance, Submission No. *114*, p. 7.

Recommendation 5

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.

Standardise warrant tests and thresholds

2.55 In its submission to the Committee, the AGD addressed possible changes to the tests for telecommunications interception warrants, specifically the threshold at which interception warrants are available:

> Warrants relating to accessing real-time content are traditionally limited to investigating an offence that carries a penalty of at least seven years imprisonment: a 'serious offence' as defined in section 5D of the TIA Act. Section 5D is an exhaustive list which includes offences by reference to other Commonwealth legislation (such as an offence against Part 10.7 of the Criminal Code Act 1995) or of a certain type (such as murder) or involving certain conduct (such as trafficking in prescribed substances) all of which generally require at least seven years imprisonment.
>
> …
>
> The Department considers that these requirements should not change: access to real-time content should continue to be subject to an independently issued warrant for the investigation of a serious offence.
>
> …
>
> The Department is concerned that the growing complexity of section 5D of the TIA Act is inefficient in terms of police resources needed to clarify the application of the provision in specific circumstances and, more importantly, potentially privacy invasive in its lack of clarity about how and …
>
> The Department considers that the interception regime would offer greater privacy protection if the distinction between stored and live warrants was removed and if a standard threshold for both content and stored communications warrants was introduced.[46]

2.56 The issue of a standard threshold for TIA Act warrants attracted significant evidence for the Committee's consideration. Many submitters acknowledged the potential administrative efficiencies to be gained from standardisation, but

46 Attorney-General's Department, *Submission No. 218*, p. 5.

objected to the potential for warrant thresholds to be lowered. For example, Liberty Victoria submitted:

> Standardisation of interception warrant tests must not compromise human rights – Liberty Victoria recognises that there may be operational benefits in standardising various warrant tests. However, we are concerned to ensure that any standardisation process does not compromise human rights in the name of operational efficiencies. In particular, we oppose any reduction of the general threshold for interception so that it applies to offences with maximum penalties of less than 7 years' imprisonment.[47]

2.57 The Committee also received extensive evidence from law enforcement agencies regarding the complexity of the present threshold for telecommunications interception warrants. For example, Victoria Police submitted:

> The definition of serious offence pursuant to section 5D of the TIA Act is long, complex and outdated and it excludes offences which should be so classified. There are offences Victoria Police routinely investigates that are serious in nature, but are not specified in the definition or only become serious offences if they meet certain additional conditions such as being part of a series of offences, involve substantial planning and organisation and sophisticated methods and techniques.
>
> Offences that are serious in nature but are not captured in this section include blackmail and perverting the course of justice, where an investigative method such as telecommunications interception would assist in the investigation of offenders charged with serious crimes attempting to arrange false alibis or have witnesses change their statement and/or provide false evidence.[48]

2.58 Similarly the Western Australia Police submitted:

> At present, under the TIA Act, it is not possible to obtain an interception warrant with respect to offences which carry a penalty of less than 7 years imprisonment but which may be preparatory to more serious offending. For example, precursor or preparatory crimes could include selling unregistered firearms, pervert the course of justice or stealing a motor vehicle. The ability to intercept communications in relation to precursor offences may assist in the prevention of more serious offending.
>
> WA Police would welcome an examination of the current definition of serious offence and serious contravention contained in the TIA Act

47 Liberty Victoria, *Submission No. 143*, p. 2. See also Mr Bernard Keane, *Submission No. 117*, p. 4; Electronic Frontiers Australia, *Submission No. 121*, p. 13; Pirate Party Australia, *Submission No. 134*, p. 12; and Ms Stella Gray, *Submission No. 152*, p. 8.

48 Victoria Police, *Submission No. 200*, p. 7.

> (section 5D and section 5E). The current definition is complex and unwieldy, and requires simplification.[49]

2.59 The appropriate threshold for access to the content of communications is a complex issue. As noted by the Australian Competition and Consumer Commission, stored communications warrants are available for pecuniary penalty offences in addition to the threshold set by a period of imprisonment:

> In the main, telephone interception is limited to investigation of serious offences under criminal law where the conduct is punishable by seven years' imprisonment or more. In contrast, stored communications warrants can be issued by a judge for serious contraventions of civil or criminal law involving a fine or pecuniary penalty equivalent to at least $19,800 (individuals) or $99,000 (businesses), as well as for serious criminal offences capable of interception.[50]

2.60 Rather than lowering the existing threshold, the Law Council of Australia advocated lifting the relevant thresholds:

> The Law Council is of the view that it is appropriate for the offence threshold for stored communication warrants to be reviewed and raised to apply only to criminal offences. Consideration should also be given to raising this threshold to 'serious offences', as defined in section 5D of the TIA Act, in recognition of the private nature of stored communication information and to better align the stored communication warrant process with that required for telecommunication interception warrants.[51]

2.61 As stated by the Inspector-General of Intelligence and Security, 'proposals to standardise security warrant tests and thresholds must take into account the nature of each of these warrants and the level of intrusiveness.'[52]

2.62 The Committee notes that there are differing penalty thresholds within the TIA Act, and between the TIA Act and other electronic surveillance powers (such as the *Surveillance Devices Act 2004*). The appropriate threshold for access to telecommunications and access to stored communications (whether they be combined under a single test) requires a careful consideration of the:

- proportionality of the investigative need and the privacy intrusion;
- gravity of the conduct to be investigated by these investigative means;
- scope of the offences included and excluded by a particular threshold;

---

49 Western Australia Police, *Submission No. 203*, p. 8.

50 Australian Competition and Consumer Commission, *Submission No. 192*, p. 5.

51 Law Council of Australia, *Submission No. 96*, p. 30.

52 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 9.

- impact on law enforcement agencies investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences; and
- privacy impact.

2.63 The Committee is not able, upon the evidence before it, to reach a final position about the appropriate threshold for access to telecommunications and stored communication. Rather, the Committee is attracted to the proposal from the AFP for a further review to consider this issue:

> The appropriateness of these separate warrant tests and offence thresholds should be reviewed taking into consideration the contemporary use of communications in society generally and by persons of interest in the commission of crime, and the nature of the technology underpinning telecommunications and internet communication services. A key example of this is the increasing use of stored communication as a means of covert communication.
>
> From a law enforcement perspective such a review needs to take into account the basis of the gravity of the conduct; the increasingly ubiquitous nature of telecommunications content and stored communications as evidence of the commission of an increasing number of offences that cause significant harm to the community, and the transitory nature of that content. It may be that the differentiation currently imposed between the two forms of content is no longer appropriate and that a reviewed and unified threshold would be more appropriate to meet both community expectations and law enforcements needs.[53]

2.64 The Committee notes that telecommunications interception warrants may be issued for the investigation of offences with a maximum penalty of at least seven years imprisonment but stored communications warrants may be issued for the investigation of offences with a significantly lower threshold of at least three years imprisonment as a maximum penalty. There is arguably very little difference in the privacy impact carried out if communications are accessed live via interception or after the communication takes place when accessed with a stored communications warrant. The Committee is of the view that covert access to communications should not distinguish between access methods, and that therefore the penalty threshold should be standardised.

53 Australian Federal Police, *Submission No. 163*, pp. 9-10.

Recommendation 6

The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the:

- **privacy impact of the threshold;**
- **proportionality of the investigative need and the privacy intrusion;**
- **gravity of the conduct to be investigated by these investigative means;**
- **scope of the offences included and excluded by a particular threshold; and**
- **impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.**

Expanding the basis of interception activities

2.65 The AGD discussion paper describes the challenge to the ongoing effectiveness of telecommunications interception as follows:

> Telecommunications interception and access to communications data are unique and fundamental tools that cannot be replaced by other investigative techniques. They are cost effective, timely, low risk and extremely successful tools in obtaining intelligence and evidence. Substantial and rapid changes in communications technology and the business environment are rapidly eroding agencies' ability to intercept. Adapting the regime governing the lawful access to communications is a fundamental first step in arresting the serious decline in agencies' capabilities.[54]

2.66 The Committee notes the effectiveness of telecommunications interception as an investigative technique. The *Telecommunications (Interception and Access) Act 1979 Annual Report for 2010-11* notes that intercepted information contributed to 2441 arrests, 3168 prosecutions, and 2034 convictions for the 2010-11 financial year.[55]

2.67 The Committee took evidence on the decline in agencies' interception capability, referred to as 'going dark':

---

54 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 23.

55 Telecommunications (Interception and Access) Act 1979 Annual Report 2010-11, pp. 42, 44-5.

> In terms of this concept of going dark, it is certainly something that is being increasingly discussed amongst the law enforcement fraternity and it is a recognition primarily of these new technologies that we are unable to intercept for a range of reasons. That is one of the areas that I would respectfully suggest that the committee needs to consider in terms of the ongoing viability of telecommunications interception generally.[56]

2.68 The AFP submitted that the telecommunications environment has shifted considerably since 1979 resulting in significant challenges to interception:

> That industry environment no longer exists. Several service or application providers may be involved in any one communication event. Individuals often use multiple devices and applications to communicate and free accounts can be established quickly and with no clear connection to a real life identity. Further, the current approach presupposes that the communications are between people using devices, not machine based communications as may be used through botnets or other internet based crimes where communications content is an important source of evidence. Into the future, given the move from circuit based to IP based telecommunication services, identifying communications between persons will become increasing challenging.
>
> In light of this it is no longer viable to continue to base interception solely on the traditional network identifiers prescribed in the TIA Act. For this reason the AFP considers additional bases for interception such as the concept of communications of interest that relate to the offence under investigation would be of benefit. This concept could include the source of a communication, the destination of a communication, and the type of communication.[57]

2.69 The Committee heard evidence that a proposal for 'attribute based interception' would assist in countering the decline of capability caused by technological and counter-security measures. The Western Australia Corruption and Crime Commission explained the proposal:

> Being able to identify particular communications within the service, for example, may allow agencies to exclude or include particular communications through relevant identifiers. For example, if an internet based interception were to be conducted on a user's account the agency may only be interested in particular communications such as those linked to an email address or internet chat protocol. By expanding the basis for interception activity, agencies may be able to exclude other

56 Detective Inspector Gavan Seagrave, *Transcript*, 5 September 2012, pp. 29-30.

57 Australian Federal Police, *Submission No. 163*, pp. 12-13.

> communications thereby better targeting the communications of interest and providing greater privacy protection by excluding other content.[58]

2.70 A range of submissions noted the potential privacy protection which could be achieved by introducing a warrant which better targeted communications on the basis of specific attributes. Those submissions noted however the need to ensure appropriate oversight and accountability of the proposed warrant type:

> The Law Council recognises the challenges existing and emerging telecommunications technologies pose for agencies attempting to accurately identify the communications they intend to intercept or access. For this reason, the Law Council generally supports efforts to develop a warrant regime that focuses on better targeting the characteristics of a communication and enables it to be isolated from communications that are not of interest. However, the Law Council is keen to ensure that any proposed 'simplification of the warrant process' does not occur at the expense of specific provisions designed to ensure that each particular device or service to be intercepted or communication to be accessed is clearly identified and shown to be justifiable and necessary, and that it occurs in a manner that has the least intrusive impact on individual rights and privacy.[59]

2.71 Liberty Victoria similarly expressed in principle support subject to appropriate oversight and accountability arrangements:

> Liberty Victoria is not at this stage opposed to further consideration being given to expanding interception obligations from the network/service layer to the application layer. Interception at the network/service layer often involves casting the net of information to be intercepted too broadly, with a greater risk of capturing irrelevant and innocent communications. However, any expansion must be accompanied by the adoption of appropriate safeguards and accountability mechanisms.[60]

2.72 Other submissions expressed concern at the potential impact on privacy which may result from expanding the basis of interception:

> When viewed in the context of a proportional response to the current threat landscape I do not feel that the expansion of interception activities as outlined in the ToR and discussion paper are proportional to the massive invasion of privacy entailed. The cost to our privacy is too high in relation to a threat that if anything is subsiding and to which it appears

58 WA Corruption and Crime Commission, *Submission No. 156*, p. 10.

59 Law Council of Australia, *Submission No. 96*, p. 31

60 Liberty Victoria, *Submission No. 143*, p. 3.

> the security agencies of our nation have enough tools to combat effectively anyway.[61]

2.73 The AGD submission described the present considerations an issuing authority must address prior to issuing a telecommunications interception warrant:

> The independent authority may issue the warrant if satisfied from the facts outlined in the affidavit that:
>
> - there are reasonable grounds for suspecting that the person is using or is likely to use the service
> - that information obtained under interception would be likely to assist the investigation of a serious offence in which the person is involved
> - and having regard to:
>   - ⇒ the privacy of any persons likely to be interfered with by interception
>   - ⇒ the gravity of the conduct being investigated, and
>   - ⇒ the extent to which other methods of investigating the offence have been exhausted or would prejudice the investigation.[62]

2.74 The Committee received evidence from the Commonwealth Ombudsman and Inspector-General of Intelligence and Security. No issue of substantive non-compliance by the interception agencies was raised before the Committee. The Inspector-General of Intelligence and Security did raise, however, a range of issues for consideration should this proposal be adopted:

> A key issue to be considered in this proposal is whether the warrants would be limited to interception based on the 'characteristics' described in the initial warrant (similar to a service warrant) or whether ASIO would itself be able to vary the warrant to add or remove 'characteristics' (similar to a named person warrant). If the proposal is for the latter then there needs to be certainty as to the parameters within which 'characteristics' can be added.
>
> …
>
> A further issue is the technological capacity to actually undertake this type of 'characteristic'-based interception – including whether the carriers should be responsible for collecting, processing and delivering the communications of interest or whether the agencies should be permitted to collect and retain large amounts of information in order to find the communications of interest. It is outside my area of focus to comment on the technology, cost or burden sharing aspects of the proposal. However I would expect to see any regime include appropriate measures to ensure

---

61 Mr Daniel Judge, *Submission No. 157*, p. 9. See also J Trevaskis, *Submission No. 62*, p. 8; Mr Mark Newton, *Submission No. 87*, p. 9, and James (no further details), *Submission No. 7*.

62 Attorney-General's Department, *Submission No. 218*, Attachment A p. 1

> that the content of communications which were not the specific target of the warrant were not retained longer than necessary for 'sorting' and to ensure that such information is kept secure.
>
> One of the important accountability and oversight requirements of the current regime is the requirement that ASIO provide a report to the Attorney-General after the expiration or revocation of each warrant. The report must include details of the telecommunications service to or from each intercepted communication was made as well as the extent to which the warrant has assisted ASIO in carrying out its functions. This measure would be particularly important in maintaining oversight and accountability of any discretion to add new characteristics for interception.[63]

2.75 The Committee agrees with the need to ensure that telecommunications interception powers remain subject to appropriate accountability and oversight, including a robust system for obtaining telecommunications interception warrants from independent issuing authorities who have considered the privacy, proportionality and investigative necessity of proposed interception activities.

2.76 The Committee notes the potential for attribute based interception to assist in arresting the decline of interception capability, while also offering additional privacy protections by better targeting communications which are of particular relevance to the serious crime or national security threat which is being investigated.

2.77 Possible attributes which may be used in these warrants include:

- Time of a communication;
- Location of a communication; and
- an identifier or address that uniquely identifies a service or account.

63 Inspector-General of Intelligence and Security, *Submission No. 185*, pp. 11-12.

Recommendation 7

The Committee recommends that interception be conducted on the basis of specific attributes of communications.

The Committee further recommends that the Government model 'attribute based interception' on the existing named person interception warrants, which includes:

- **the ability for the issuing authority to set parameters around the variation of attributes for interception;**
- **the ability for interception agencies to vary the attributes for interception; and**
- **reporting on the attributes added for interception by an authorised officer within an interception agency.**

In addition to Parliamentary oversight, the Committee recommends that attribute based interception be subject to the following safeguards and accountability measures:

- **attribute based interception is only authorised when an issuing authority or approved officer is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;**
- **oversight of attribute based interception by the ombudsmen and Inspector-General of Intelligence and Security; and**
- **reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute based interception.**

Streamlining and reducing complexity

2.78 The AGD discussion paper also identified the need to reduce complexity in the lawful access regime as a driver of potential reform. As such, it sought an examination of:

- Ways to simplify the provisions that allow the various agencies to share information and cooperate;
- The removal of legislative duplication; and

- The creation of a single warrant with multiple telecommunications interception powers.[64]

Simplifying the information sharing provisions that allow agencies to cooperate

2.79 The TIA Act is drafted in prescriptive terms, based on the premise that interception is prohibited unless authorised by one of the limited exceptions. The prescriptive nature of the regime continues in the provisions which regulate the use and communication of intercepted information. The AGD Discussion paper explains:

> Information obtained under the *Telecommunications (Interception and Access) Act 1979* is subject to more rigorous legislative protections than other forms of information in an agency's possession. The provisions are detailed and complex in relation to record keeping, retention and destruction and can present a barrier to effective information sharing both within an agency and between agencies. This was not an issue when the Act was enacted and applied only to ASIO and the AFP, but with more agencies now defined as interception agencies and the national and transnational nature of many contemporary security and law enforcement investigations, effective co-operation within and between agencies is critical.
>
> Simplifying the current information sharing provisions would support co-operative arrangements between agencies and consideration could be given to the ways in which information sharing amongst agencies could be facilitated.[65]

2.80 The NSW Police argued that the prescriptive approach inhibits interagency cooperation and impedes agencies' abilities to cooperate effectively:

> Further, the access to and the subsequent use of information is framed throughout the *Telecommunications (Interception and Access) Act 1979* as one agency undertaking one investigation which will lead to a prosecution. I think that the act needs to be reformed to reflect new operational realities, including the different functions of agencies within the act and the fact that effective information sharing is a key component of successful investigations. The current information-sharing and dissemination scheme contained in the act is complex, confusing and cumbersome. The current provisions were not designed with joint agency operations in

64 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, pp. 8-9.

65 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 25.

> mind and are considered to be overly restrictive, with the default position being to prohibit communication of information that has been obtained lawfully.
>
> Whilst acknowledging privacy concerns—and we do acknowledge privacy concerns and the intrusive nature of telephone interception—a simplified, more permissive information-sharing communication model really does need to be adopted. If agencies are going to be encouraged and properly equipped to perform their functions and to cooperate effectively, then we need to be allowed to disseminate, communicate or share information where there is a legitimate reason to do so. Naturally, appropriate oversight and safeguards need to be and must be incorporated in such a scheme. But, overall, it is the agencies that readily use this legislation that I think are best placed to assist in its reform and the New South Wales Police Force is in an excellent position to provide further input from an operational perspective.[66]

2.81 The NSW Police supported the argument for reform with the following examples of current operational impediments:

> As an example, if we were tapping a telephone and, as a result of some information which came across that phone, we had concerns that someone was carrying a firearm on the street but we were not in a position to take any action, we cannot post that intelligence on a warning system for our officers. We would like to be able to put out a warning saying, 'If you pull this vehicle over with that person driving, be careful—intelligence suggests that they are armed.'
>
> Another example might be where we have an interception operation running and, as a result of that, we come across some information about a child abuse situation. In that setting, we are not at liberty even to advise a child protection authority that there is a telephone interception running. That is because we are not able to use that lawfully intercepted information. That is difficult. We encounter that every day.[67]

2.82 Victoria Police submitted the current TIA Act regime is too restrictive, and inhibits community protection:

> While it is important that there are strict controls over the sharing of information, Victoria Police investigators have on occasion found the legislation to be too restrictive. There have been instances where lawfully intercepted information would be of high importance to other organisations providing a function in the service of the community, but

66 Commissioner Andrew Scipione, *Transcript*, 26 September 2012, pp. 17-18. See also Western Australia Police, *Submission No. 156*, p. 6.

67 Commissioner Andrew Scipione, *Transcript*, 26 September 2012, p. 25.

> Victoria Police is legislatively prevented from providing it. For example, if an interception identifies that a child is at risk of harm from its parents, this information cannot be communicated to child protection agencies. Similarly, where investigators identify the inappropriate dealings of a prison officer, this information cannot be passed on to prison authorities.[68]

2.83 A number of submissions noted in-principle support for streamlined information sharing provisions, citing the need for effective collaboration between law enforcement and national security agencies. That support, however, was subject to concerns that simplified information sharing provisions should not intrude upon privacy to any extent greater than is necessary for the purpose of the investigation. The Liberty Victoria submission is illustrative in this regard:

> Liberty Victoria acknowledges that there is an increasing need for agencies defined as 'interception agencies' – including those responsible for national and transnational security and law enforcement investigations – to share information with one another. The nature of transnational security concerns means that agencies other than ASIO and the Australian Federal Police (AFP) are involved in investigations which impact the security of Australia, as well as Australian citizens within Australia and abroad.
>
> However, as noted above in relation to standardisation of the tests and thresholds relating to warrants, detailed information-sharing provisions may reflect a desire to appropriately balance the right to privacy against security considerations. Careful consideration will therefore need to be given about whether the complexity of information-sharing provisions is justified. In Liberty Victoria's view, any broadening of scope to allow additional information-sharing between agencies should be taken seriously and with the upmost concern for privacy. Again, while Liberty Victoria recognises the need to facilitate information-sharing between agencies in some cases, there is insufficient detail in the Discussion Paper for stakeholders to comment in detail.[69]

2.84 Similarly, Ms Stella Gray expressed concern that streamlined information sharing did not become unregulated information centralisation:

> It is fair and reasonable to assume that if an agency obtains evidence of a crime that is outside their jurisdiction to pursue, they should be able share that evidence with the relevant agency. However, they should only share the evidence relevant to the crime in question. If agencies were allowed to share the entirety of communications intercepted under the original warrant, this would be a clear case of overreach, and has severe

68 Victoria Police, *Submission No. 200*, p. 11. See also Western Australia Police, *Submission No. 203*, p. 9.

69 Liberty Victoria, *Submission No. 143*, pp. 8-9.

> implications for citizens' privacy. It is crucial that all information gathered from warrants remains stored separately as a privacy safeguard. If this aspect of information sharing is not treated with precision, there will be a temptation to create a central database accessible by all agencies, which is a security and privacy risk in itself.[70]

2.85 Mr Bernard Keane submitted that the case for simplified information sharing had not been made:

> The argument that information should be more easily shared between agencies is a glib one, and the only justification advanced in the paper is that 'effective co-operation within and between agencies is critical.' This of course is assertion rather than argument; no effort is made by AGD to explain what failings are currently occurring because of the legislative restraints on his intercepted data can be shared.
>
> …
>
> AGD has offered no justification for violating the long-standing philosophy that intercepted information should only be used for the purposes for which it was collected, rather than becoming a common treasure trove to be dipped into by all law enforcement and intelligence agencies at will.[71]

2.86 The Pirate Party Australia expressed support for enhanced reporting, but did not support a reduction in accountability:

> We support security agencies providing more relevant information about the proportionality of any use of their invasive powers, while opposing any streamlining that reduces the ability of investigative bodies to uncover corruption or abuse of power.[72]

2.87 The AFP submission included several case studies to illustrate that the current prescriptive information sharing provisions impede operational collaboration. The AFP stated:

> The complex and evolving nature of transnational crime means that no one agency can effectively conduct complex investigations. Collaboration is an essential element in achieving operational goals. The TIA Act as it currently stands impedes the effective exchange of lawfully obtained communications information and reduces the efficiency of operational partnerships. Simplified, principle based use and disclosure rules would be more consistent with the modern approach to cooperation between

70 Ms Stella Gray, *Submission No. 152*, p. 7.

71 Mr Bernard Keane, *Submission No. 117*, p. 4.

72 Pirate Party Australia, *Submission No. 134*, p. 13.

> agencies and assist in assuring information obtained under lawful interception is maximised appropriately to serve the public good.[73]

2.88 The Office of the Australian Information Commissioner acknowledged the necessity of information sharing to effective investigative collaboration, but noted the need to ensure clarity of obligations and standards regarding the protection of the privacy of personal information due to fragmented information handling obligations:

> [t]he OAIC considers that this fragmentation makes it particularly important that each of the applicable regulatory frameworks setting out information sharing arrangements between law enforcement and intelligence agencies clearly and consistently specifies the nature, scope and limits of the information sharing activities. This includes specifying what protections are afforded to any personal information collected, used or disclosed under the information sharing arrangement.[74]

2.89 Mr Newton noted general support for information sharing simplification, but not if it resulted in a net reduction in privacy protections:

> In particular, I would not support a sharing regime which enabled an agency which had obtained evidence for a certain purpose to divulge it to a second agency for a different purpose, if that second agency would otherwise be required to obtain their own warrant.[75]

2.90 The Law Council of Australia submitted it is appropriate that information obtained under the TIA Act is subject to more rigorous legislative protections than other forms of information in a law enforcement agency's possession:

> Sharing this type of information must necessarily be more restricted than sharing other information in order to recognise its particularly sensitive nature and the intrusive impact on a person's rights and privacy. It could include, for example, details of a person's most private conversations or the precise location of a person, and may include information in relation to non-suspects or other innocent third parties. Provisions relating to the sharing of this type of information must also reflect limits on the types of officers who are able to have primary access to this information.[76]

2.91 Rather than simplification to enable greater interagency information sharing, the Law Council suggested reforms should look at 'strengthening and clarifying the existing provisions, recognising that different restrictions on communication, use and disclosure may be appropriate in light of the nature of the information

---

73 Australian Federal Police, *Submission No. 163*, p. 10. See also: Australian Customs and Border Protection Service, *Submission No. 168*, p. 3.

74 Office of the Australian Information Commissioner, *Submission No. 183*, pp. 10-11.

75 Mr Mark Newton, *Submission No. 87*, p. 7.

76 Law Council of Australia, *Submission No. 96*, p. 46.

obtained, and depending on what types of agencies are able to have primary access to such information.'[77]

2.92 The Committee supports the need to ensure that any amendments to the information sharing provisions provide appropriate privacy protections. The Committee understands, however, one of the potential benefits of proposed information sharing reforms is to enable investigative agencies to provide intercepted information to an agency that is responsible for investigating particular criminal activity.

2.93 The Committee supports the view that information sharing provisions should continue to impose appropriate restrictions upon the use and disclosure of telecommunications interception information, having regard to its privacy intrusive nature. The Committee also supports the need for law enforcement and security agencies to be able to share information to ensure that serious crimes and threats to national security can be investigated in a timely and thorough manner.

2.94 The Committee is concerned about the proliferation of institutions that gather and share information, and the absence of consistent guidelines and sufficient oversight.

Recommendation 8

The Committee recommends that the Attorney-General's Department review the information sharing provisions of the *Telecommunications (Interception and Access) Act 1979* to ensure:

- **protection of the security and privacy of intercepted information; and**
- **sharing of information where necessary to facilitate investigation of serious crime or threats to national security.**

Removing legislative duplication

2.95 The discussion paper notes that legislative complexity has been created by frequent amendments to the TIA Act:

> The pace of change in the last decade has meant the Act has required frequent amendment resulting in duplication and complexity that makes

77 Law Council of Australia, *Submission No. 96*, p. 47.

> the Act difficult to navigate and which creates the risk that the law will not be applied as Parliament intended.[78]

2.96 The Attorney-General's Department was asked on notice to provide examples of legislative duplication. The Department noted that it considers that the multiple types of warrants are no longer appropriate for the modern communications landscape:

> Key areas of duplication relate to the different types of warrants, including the distinction made between intercepted and stored communications.[79]

2.97 The Department observed that the duplicated nature of warrants leads to other forms of unnecessary legislative duplication:

> The oversight, record keeping and reporting provisions which flow from these warrant provisions are also duplicative. For example, in relation to oversight responsibilities, there is dual oversight of State and Territory agencies by both the Commonwealth Ombudsman and the relevant State or Territory oversight agency.
>
> In relation to record keeping and reporting, there are three separate annual report requirements for telecommunications interception warrants, stored communication warrants and access to telecommunications data. In the case of interception warrants there are separate annual report requirements for Commonwealth agencies and State prescribed authorities, there are also two separate reporting requirements for State agencies. The three requirements differ making it difficult to undertake a meaningful analysis and comparison of the different mechanisms. [80]

2.98 The Department presented the overall view that:

> …streamlining and modernising lawful access to telecommunications provisions through the creation of a one warrant regime that regulates access to the content of a communication, together with the flow on effects to the oversight, record keeping and reporting requirements, will remove significant duplication and complexity from the TIA Act and create consistency in the accountability framework.[81]

2.99 The Committee is of the view that removing legislative duplication would help to make the interception regime easier for the general public, legal practitioners, law enforcement and the justice system to understand and apply.

---

78 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 17

79 Attorney-General's Department, *Submission No. 236*, p. 18.

80 Attorney-General's Department, *Submission No. 236*, p. 18.

81 Attorney-General's Department, *Submission No. 236*, p. 18.

Recommendation 9

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to remove legislative duplication.

A single warrant with multiple telecommunications interception powers

2.100 The AGD submission states:

> The Department considers that the interception regime would offer greater privacy protection if the distinction between stored and live warrants was removed and if a standard threshold for both content and stored communications warrants was introduced. Reliance on the higher seven year penalty threshold has not proved successful in limiting the application of interception powers. On the other hand the three year stored communications threshold underestimates the value of non-voice communications in the contemporary communications environment. A threshold in between these two would recognise the growing importance of non-voice communications and enable interception to be used as a tool in investigating a number of serious crimes that currently fall outside the TIA Act.
>
> A single warrant, and clarification of the concept of serious offence, would greatly enhance the capacity of the interception regime to ensure that interception is only available in defined circumstances.[82]

2.101 Victoria Police supported the proposal for a single warrant, noting in its submission:

> It is no longer practicable for warrants to be obtained solely on traditional network identifiers such as telephone numbers or International Mobile Equipment Identifier (IMEI) numbers. A single warrant in which particular identifier(s) could be stipulated (such as a username, webmail address, internet account) would enable the targeting of communications of a suspect without the need for multiple warrants over time on the same target.[83]

2.102 Similarly, the Western Australia Police expressed support for the efficiency and flexibility a single warrant regime would represent:

82 Attorney-General's Department, *Submission No. 218*, p. 5.

83 Victoria Police, *Submission No. 200*, p. 13.

> The creation of a single warrant with multiple TI powers would provide the flexibility to cater for future technological change by having a focus on communications made by an individual rather than the specific technology or equipment used.
>
> WA Police is of the view that the use of a single broad based warrant would simplify an otherwise overly complicated regime. At present, the TIA Act provides for 6 different warrants (service warrant, b-party interception warrant, named person warrant, device based interception warrant, section 48 entry onto premises warrant, stored communications warrant), each of which have specific applicability. The application of the current warrant regime has the potential to cause confusion as police officers are often unsure about which warrant best suits the needs of a particular investigation.[84]

2.103 The Australian Mobile Telecommunications Association – Communications Alliance joint submission noted reservation with the proposal for a single warrant due to the potential for it to shift obligations and due diligence checks onto telecommunications providers:

> A telecommunications service provider must be able to clearly determine from the warrant which services should be intercepted in order to properly implement a warrant. For these same reasons the responsibility to identify relevant services should rest with the intercepting agency and not the service provider. Industry also expects that there will be a continuing need for independent oversight of warrant applications prior to them being served on a carrier or carriage service provider. It would not be possible for the oversight process to fully assess the impact of each warrant if the carrier or service provider is subsequently required to make the decisions about what particular services are to be intercepted.[85]

2.104 Similarly, iiNet noted the need for warrants to avoid shifting questions of judgement to telecommunications providers:

> The Discussion Paper does not specify what the particular 'TI powers' will be (i.e. whether a consolidation of existing powers is intended or the addition of new powers). iiNet believes that it is important that it be recognised that C/CSPs are not State agents, and a clear demarcation should be maintained between CSPs providing access and C/CSPs doing more than providing access. Furthermore, C/CSPs should not be required to make any judgement calls as regards what particular information is

84 Western Australia Police, *Submission No. 203*, p. 11.

85 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 10.

> required for a C/CSP to comply with a warrant. Therefore, warrants should contain clear and specific terms.[86]

2.105 Interception agencies explained to the Committee, however, that the proposal for a single telecommunications interception warrant would significantly increase administrative efficiency without diminishing accountability:

> The current TIA Act requires various types of warrants to access communications lawfully. Additional types of warrants have been created over the years in response to changes in methodologies and technologies. The resultant system is complex requiring detail to be interpreted by agencies, issuing authorities, oversight bodies, and courts. The Commission supports the concept of a single simplified warrant. The relevant thresholds and privacy intrusions are essentially the same where communications are accessed via service device be they stored communications or intercepted in transit. [87]

2.106 A number of submissions expressed cautious support for the proposed single warrant, noting the potential for efficiencies within the warrant process, but noted concern at the potential for the proposal to diminish thresholds. The Pirate Party submission is an example of this position:

> If this single warrant retains a threshold test for serious crimes (with a penalty of 7 years or greater imprisonment) then there should be no obstacle in implementing it. If, however, the threshold is lower than that then there would be grave concerns in allowing it.[88]

2.107 The Tasmanian Association of Community Legal Centres expressed concern the proposal would lead interception agencies to using available powers, rather than the most appropriate power:

> In our view the current legislative requirement that law enforcement agencies apply for either a 'telecommunications service' warrant (authorising the interception of only one service, such as a single telephone number) or a 'named person' warrant (authorising the interception of any telecommunication services or devices that are likely to be used by the person named in the warrant) reduces the risk that law enforcement agencies will use all the powers available to them rather than being used for a specific purpose as currently provided in the powers of the two warrants.[89]

2.108 The issue of the thresholds and how to deliver the appropriate accountability was usefully addressed by the Inspector-General of Intelligence and Security:

86 iiNet, *Submission No. 108*, p. 10.

87 Western Australia Corruption and Crime Commission, *Submission 156*, p. 8.

88 Pirate Party, *Submission No. 134*, p. 15.

89 Tasmanian Association of Community Legal Centres, *Submission No. 184*, pp. 2-3.

> Having multiple sets of warrant applications for a single investigation is administratively inconvenient for ASIO and does not necessarily provide the Attorney-General with a clear view of the totality of proposed activities. Any proposal to streamline this and give the Attorney-General a better picture of the situation is worthy of consideration but issues of proportionality and levels of authorisation will need careful consideration.
>
> …
>
> One interpretation of the proposal in the discussion paper could be that the Attorney-General is to be asked only to agree broadly to 'interception' against a particular individual, group or premises for a specified period and to then allow the Director-General of Security or a delegated ASIO officer to decide what form that interception should take during the warrant period (including whether B-Party interception is appropriate). I note that a 'named person warrant' currently allows the Director-General of Security to add or remove services from interception coverage during the life of the warrant to enable interception of communications made by or to the specified individual. Any proposal to effectively further transfer the level of decision making from Ministerial level to within an agency needs to ensure that appropriate reviews take place within the agency, make allowance for independent scrutiny and consider external reporting requirements.[90]

2.109 Similarly, the Gilbert + Tobin Centre for Public Law noted the need to ensure that a regime for a single telecommunications interception warrant should continue to ensure proportionality is considered by the issuing authority:

> The most recent report of the Attorney-General's Department into the operation of the TIA Act states that a named person warrant has a 'high impact on privacy'. It should only be used 'when necessary and other alternative methods are not available'. Therefore, in the majority of cases, law enforcement agencies obtain a telecommunications service warrant rather than a named person warrant. This is the correct approach. Any intrusions into the right to privacy should be the minimum required to achieve the public purpose. We are concerned that merging of named person warrants and telecommunications service warrants into a single category of warrant would result in law enforcement agencies using all the powers that are available to them (regardless of whether these powers are strictly necessary to investigate the criminal activity).[91]

---

90 Inspector-General of Intelligence and Security, *Submission No. 185*, pp. 9, 10.

91 Gilbert + Tobin Centre for Public Law, *Submission No. 36*, p. 9.

2.110 The Law Council of Australia also noted reservations about the proposal's potential to diminish accountability, particularly in the absence of detail within the Attorney-General's Department Discussion Paper. The Law Council helpfully indicated some of the considerations which could be addressed if the reform were to be supported:

> However, if a proposal of this nature were pursued, the Law Council would suggest that the issuing authority must be satisfied of the following minimum requirements:
>
> - that any person whose telecommunications are to be intercepted is specifically identified as a legitimate target of suspicion from a security or law enforcement perspective;
> - that each and every telecommunications service or telecommunications device to be intercepted is, in fact, used or likely to be used by the relevant person of interest; and
> - each and every telecommunications service or telecommunications device to be intercepted can be uniquely identified such that relevant telecommunications made using that service or device can be isolated and intercepted with precision.
>
> In addition, the issuing officer should also have regard to:
>
> - the likely benefit to the investigation which would result from the intercepted information substantially outweighing the extent to which the interception is likely to interfere with the privacy of any person or persons;
> - the gravity of the conduct constituting the offence or offences being investigated;
> - how much the information referred to would be likely to assist in connection with the investigation by the agency of the offence or offences; and
> - to what extent methods of investigating the offence or offences that do not involve intercepting communications have been used by, or are available to, the agency[92].

2.111 The Committee acknowledges the need to ensure that intrusive investigative techniques are exercised only in necessary and justified circumstances, and that the intrusion is proportionate to the conduct being investigated. A balance must be struck between appropriate checks and balances, and the operational flexibility required to deliver effective law enforcement and protection against national security threats.

2.112 The Committee is of the view that revising the present multiple telecommunications interception warrants into a single warrant regime can deliver administrative efficiencies to interception agencies without removing

92 Law Council of Australia, *Submission No. 96*, p. 53.

appropriate accountability and safeguards.

Recommendation 10

The Committee recommends that the telecommunications interception warrant provisions in the *Telecommunications (Interception and Access) Act 1979* be revised to develop a single interception warrant regime.

The Committee recommends the single warrant regime include the following features:

- **a single threshold for law enforcement agencies to access communications based on serious criminal offences;**
- **removal of the concept of stored communications to provide uniform protection to the content of communications; and**
- **maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises.**

The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures:

- **interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;**
- **rigorous oversight of interception by the ombudsmen and Inspector-General of Intelligence and Security;**
- **reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and**
- **Parliamentary oversight of the use of interception.**

Modernising the cost sharing framework

2.113 The final area for potential legislative reform identified by the AGD discussion paper relates to modernising the cost-sharing framework. The discussion paper provided by the AGD proposes that cost sharing frameworks be modernised by aligning 'industry interception assistance with industry regulatory policy' and by

clarifying the role of the Australian Communications and Media Authority's role in regulation and enforcement.[93]

Align industry interception assistance with industry regulatory policy

2.114 The terms of reference to this inquiry state the Government wishes to progress the modernisation of the cost-sharing framework to align industry interception assistance with industry regulatory policy. The industry assistance obligations are contained in the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and in the *Telecommunication Act 1997*. The discussion paper explains:

> In reforming cost sharing, consideration must also be given to the current make-up of the telecommunications industry. The current requirements are predicated on the existence of one or few industry players and assume that all are resourced on a similar basis and have a similar customer base. This does not reflect industry practice which better suits a tiered model that supports comprehensive interception and delivery capability on the part of larger providers, a minimum interception and delivery capability on the part of medium providers and only reasonably necessary assistance for interception on the part of smaller providers.
>
> A tiered model would also recognise that smaller providers generally have fewer customers and therefore have less potential to be required to execute an interception warrant and less capacity to store and retain information about communications and customers.[94]

2.115 The Department explained that the current cost responsibility principles for the maintenance of effective were established following the 1994 review into the *Long term Cost-effectiveness of Telecommunications Interception* by Mr Pat Barrett.[95] The Department also gave an example of a more flexible approach to applying obligations to the contemporary telecommunications environment:

> The requirement for all industry participants to have the same interception capability can also be an expensive and unnecessary burden that can act as a barrier to entry to the telecommunications market for new industry players. Therefore, requiring all service providers to have the same interception capability regardless of size (as in the current system) could have the effect of restricting competition rather than promoting it and stifling innovation (noting that the promotion of the

93 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 13.

94 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 28.

95 Attorney-General's Department, *Submission No. 236*, p. 19.

> supply of diverse and innovative carriage services and content services is one of the objects of the Telecommunications Act).[96]

2.116 The Department concluded:

> The current industry and legislative cost allocation framework is working well, but efficiencies may be able to be made in regards to standardisation of technical and administrative requirements in meeting these obligations. Opportunities for reducing red tape and achieving regulatory offsets may also be identified.[97]

2.117 The Committee appreciates that the telecommunications environment has evolved rapidly and is significantly different in size, composition and international presence to the industry that existed when the TIA Act was first passed.

2.118 Therefore, the Committee agrees that there is merit in reconsidering application of the cost-sharing provisions of the telecommunications interception regime to provide a more flexible approach.

Recommendation 11

The Committee recommends that the Government review the application of the interception-related industry assistance obligations contained in the *Telecommunications (Interception and Access) Act 1979* and *Telecommunications Act 1997*.

Clarify ACMA's regulatory and enforcement role

2.119 The Australian Communications and Media Authority (the ACMA) has the following functions and responsibilities:

> The Australian Communications and Media Authority (ACMA) is a government agency responsible for the regulation of broadcasting, the internet, radiocommunications and telecommunications.
>
> The ACMA's responsibilities include:
>
> - promoting self-regulation and competition in the communications industry, while protecting consumers and other users
> - fostering an environment in which electronic media respect community standards and respond to audience and user needs
> - managing access to the radiofrequency spectrum

96 Attorney-General's Department, *Submission No. 236*, p. 19.

97 Attorney-General's Department, *Submission No. 236*, p. 19.

- representing Australia 's communications interests internationally.[98]

2.120 The AGD discussion paper suggested that the enforcement mechanisms available to the ACMA in relation to telecommunications interception regulation should be expanded:

> Consideration should also be given to clarifying the role of the Australian Communications and Media Authority (ACMA) in regulating industry obligations under the interception regime. The ACMA has rarely used its powers to enforce compliance with the TIA Act because the only effective power available to it under the Act is court action. Court action is usually inappropriate or excessive in the circumstances and unhelpful from an agency perspective because it may publicly disclose that a particular C/CSP is not complying with its TIA Act obligations. The ACMA's role could be reinforced by expanding the range of regulatory options available and clarifying the standards with which industry must comply.[99]

2.121 Telstra expressed support for clarifying the ACMA's enforcement role, also noting the need to ensure appropriate consideration is given to education and dispute resolution roles:

> Telstra believes there needs to be clarification as to what role ACMA will have in future in monitoring compliance by C/CSPs with the Telco Act and TIA Act in respect to national security and law enforcement.
>
> The Discussion Paper does not suggest what types of additional powers may be contemplated. Telstra would recommend that whatever agency is given this enforcement role its primary focus should be on undertaking an active role in education and dispute resolution, with any penalty enforcement role being secondary.[100]

2.122 Mr Ian Quick expressed opposition to the proposal due to the potential loss of transparency:

> A significant advantage of the current ACMA's power – going to court– is that it is public and open to scrutiny. If, as the discussion paper suggests –
>
> > 'The ACMA's role could be reinforced by expanding the range of regulatory options available and clarifying the standards with which industry must comply.'
>
> it would be possible – though the paper does not say what the 'options' are – that the ACMA could quietly push a C/CSP into doing something it

98 Australian Communications and Media Authority website, <www.acma.gov.au>, viewed 7 June 2013.

99 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 28.

100 Telstra, *Submission No. 189*, p. 7

> did not want to do. While this may be alleviated by clear standards, any option it has should be open to public scrutiny.[101]

2.123 The Committee did not receive a submission from the ACMA but notes the suggestion from Mr Bernard Keane to review the 2005 report *Reform of the broadcasting regulator's enforcement powers* prepared for ACMA by Professor Ian Ramsay. As Mr Keane noted:

> *Reform of the broadcasting regulator's enforcement powers* is a valuable analysis of regulatory theory that should provide the basis for an effective regulator's suite of tools for achieving effective industry regulation. … In particular, it addressed the issue of a lack of 'mid-tier' powers, which is a similar issue to that raised by AGD in the paper in relation to powers to enforce compliance with the TIA Act. On this issue, a power to accept enforceable undertakings, and a power to issue infringement notices, would appear to be two mid-tier powers worth considering to enable ACMA to enforce compliance without resorting to litigation.[102]

2.124 The Committee notes that an effective enforcement and compliance regime requires a range of sanctions and tools which are tailored to a range of potential conduct.

Recommendation 12

The Committee recommends the Government consider expanding the regulatory enforcement options available to the Australian Communications and Media Authority to include a range of enforcement mechanisms in order to provide tools proportionate to the conduct being regulated.

Requirements for industry interception obligations

2.125 The AGD discussion paper outlines the current situation regarding the expression of industry interception obligations:

> The TIA Act places an obligation on each C/CSP to have the capability to intercept communications and requires carriers and nominated carriage service providers to submit an annual interception capability plan outlining their strategy for complying with their obligation to intercept and to deliver communications to interception agencies. The obligation extends to maintaining the capability to intercept communications that

101 Mr Ian Quick, *Submission No. 95*, p. 7.

102 Mr Bernard Keane, *Submission No. 117*, p. 5.

> are carried by a service that they provide and to deliver those communications to the requesting agency consistent with a warrant.
>
> However, as networks have become more complicated and the types of services available have expanded, often beyond the C/CSPs' own networks, challenges have evolved in applying a general obligation. Consideration should be given towards introducing measures that implement more specific technical requirements to cater for a diverse and sophisticated telecommunications environment. This includes developing requirements around administrative needs such as the timeliness of cost sharing to agencies and the security measures to be applied to the handling of sensitive information relating to interception operations. [103]

2.126 The Australian Mobile Telecommunications Association – Communications Alliance supported a 'high level set of requirements for industry interception obligations to be clear, straightforward and reasonable.'[104]

2.127 iiNet submitted that it was unclear what was proposed, but that some clarification is necessary:

> This proposed reform appears to iiNet to be capable of being very broad. It is not expressly discussed in any detail in the Discussion Paper. Without detail of what this reform would involve, it is difficult for iiNet to provide any meaningful comment, except to say that there should be thorough consultation with industry on these detailed requirements. iiNet believes that consideration of any such reform should include giving consideration to clarifying the scope of section 313 of the Telco Act. The scope of the obligation to 'give such help as is reasonably necessary' is vague and uncertain.[105]

2.128 The Western Australia Corruption and Crime Commission expressed support for the potential benefits to be derived from clearly articulated obligations:

> The current regulatory regime for industry interception obligations is administratively burdensome for both industry participants and the regulatory agency. The current requirement of industry to prepare and submit interception capability plans which are then assessed annually should be reviewed.
>
> The implementation of detailed requirements for industry interception obligations may assist in clarifying requirements and account for technical

103 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 27.

104 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 10.

105 iiNet, *Submission No. 108*, pp. 10-11.

> complexities. The Commission endorses the inclusion of administrative requirements as part of industry interception requirements. In many cases, difficulties or delays in interception are due to administrative, as opposed to, technical limitations.[106]

2.129 The Committee notes that while, in general, a cooperative relationship exists between telecommunication companies and law enforcement and national security agencies, a uniform level of cooperation does not exist across all sectors of the industry. The Committee sees benefit in providing detailed guidance on the obligations imposed on the telecommunications industry to ensure telecommunications providers and interception agencies alike understand the extent of those obligations.

Recommendation 13

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to include provisions which clearly express the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data.

Clarify that the interception regime includes ancillary service providers

2.130 Although expressed as 'extending' the interception regime to ancillary service providers such as Facebook, Google and Twitter, the purpose of this term of reference is in fact to clarify that — as the Committee understands to be the case — the existing obligations do apply to ancillary service providers. It is not an extension of existing obligations.

2.131 Although he does not refer to ancillary service providers by name, Commissioner Scipione of the NSW Police Service described the challenges to national security services and the law enforcement community posed by technological change:

> A further significant challenge for law enforcement agencies investigating national security and serious criminal matters is the increasing use of sophisticated technologies by criminals. Frankly, organised criminals are now able to operate outside the reach of ordinary telecommunications interception and law enforcement agencies that are dealing with criminals who have access to unprecedented advancements in technology. Legislation that not

106 Western Australia Corruption and Crime Commission, *Submission No. 156*, p. 8.

> only fails to adequately recognise this but significantly fails to future proof itself against rapidly emerging technologies is what we are dealing with here.[107]

2.132 The rationale for clarifying the regulatory obligations of ancillary service providers under the TIA Act was stated by the Western Australia Police:

> When communication systems were conducted over telephone networks only, as was the case when the TIA Act was written, there was no question as to who was responsible for supplying the interception points. It is no longer simply the case of going to just one telecommunications provider to intercept a persons' communications. It is now quite feasible for someone to be subscribed to one provider for their telephone traffic and another provider for their Internet. Further, other providers might provide a Voice Over IP (VOIP) telephone service which then utilises a network, or multiple networks of multiple providers to get from point a to point b.
>
> Intercepting an individual's communications is no longer a simple exercise of only going to the major identified service providers. Regardless of the provider, it should be possible to intercept related Internet traffic for the purposes of investigating serious criminal activities.[108]

2.133 Victoria Police also submitted that the fact that the existing regime applied to ancillary service providers should be made clear beyond doubt:

> Monitoring of intercepted communications by Victoria Police routinely demonstrates that services such as these are being used by suspects in furtherance of their criminal activities. Without a mandatory regulatory obligation placed on the providers of these services used in Australia, criminals can continue to communicate without the risk of being exposed to interception. There needs to be legislative parity with the obligations applicable to Australian service providers.[109]

2.134 The Committee notes that the TIA Act facilitates interception and access to telecommunications data by law enforcement and national security agencies. The TIA Act facilitates this by relying upon the cooperation and assistance provided by telecommunications providers. The TIA Act does not distinguish between telecommunications providers, but provides a universal telecommunications interception obligation on all providers of telecommunications services.

---

107 Commissioner Scipione, *Transcript*, 26 September 2012, p. 18.

108 Western Australia Police, *Submission No. 203,* pp. 11-12.

109 Victoria Police, *Submission No. 200*, p. 14

2.135 Although the terms of reference requests the Committee to consider whether the existing TIA Act should 'extend' to ancillary service providers the Committee believes that the TIA Act does, under its existing provisions, include ancillary service providers. The use of the term 'extend' is inapt. The Committee received no evidence on behalf of ancillary service providers which disputed that the TIA Act applied to them. It is not an extension of existing obligations.

Recommendation 14

The Committee recommends that the *Telecommunications (Interception and Access Act) 1979* and the *Telecommunications Act 1997* be amended to make it clear beyond doubt that the existing obligations of the telecommunications interception regime apply to all providers (including ancillary service providers) of telecommunications services accessed within Australia. As with the existing cost sharing arrangements, this should be done on a no-profit and no-loss basis for ancillary service providers.

Industry participation model

2.136 The AGD discussion paper suggests the Committee should consider the merits of a tiered regime for industry assistance to intercept communications and facilitate access to telecommunications data:

> In reforming cost sharing, consideration must also be given to the current make-up of the telecommunications industry. The current requirements are predicated on the existence of one or few industry players and assume that all are resourced on a similar basis and have a similar customer base. This does not reflect industry practice which better suits a tiered model that supports comprehensive interception and delivery capability on the part of larger providers, a minimum interception and delivery capability on the part of medium providers and only reasonably necessary assistance for interception on the part of smaller providers.
>
> A tiered model would also recognise that smaller providers generally have fewer customers and therefore have less potential to be required to execute an interception warrant and less capacity to store and retain information about communications and customers. Requirements on industry to retain current information and to assist agencies to decrypt information would greatly enhance agencies' abilities to detect and disrupt criminal and other behaviours that threaten national wellbeing

> but should be implemented in a way that does not compromise business viability.[110]

2.137 Ms Stella Gray queried the efficacy of a tiered regime for industry assistance:

> A tiered interception-compliance model may simply encourage people to flock to smaller CSPs to evade surveillance, thereby negating the structure of this model.[111]

2.138 iiNet expressed in-principle support for a tiered industry assistance model, noting that it reflected industry practice:

> iiNet agrees with the comments in the Discussion Paper that a tiered model would more accurately reflect industry practice. However, iiNet believes that it is appropriate to distinguish between:
>
> - the legal obligation to provide interception capability; and
> - the manner in which that obligation is complied with by a particular C/CSP.
>
> iiNet believes that the obligation to provide interception capability should apply uniformly to all C/CSPs. However, iiNet believes that there should be flexibility as regards the manner in which a particular C/CSP complies with the obligation to provide interception capability, and the size and resources of the C/CSP should be a relevant consideration in the assessment of that C/CSP's interception capability plan.[112]

2.139 The Australian Mobile Telecommunications Association – Communications Alliance also expressed in-principle support for a tiered industry assistance model:

> Industry favours a tiered participation model, where investment in interception capabilities is based on Agency need and risk, as opposed to the current blanket obligation which requires the deployment of interception capabilities that in some cases are unlikely to be used.[113]
>
> …
>
> The current blanket approach of the TIA Act potentially gives rise to replication of interception capabilities at the carrier, wholesale service provider, retail Broadband service provider and application service layer. A more efficient regulatory framework should be sought, where replication of interception capabilities is not required.[114]

---

110 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 28.

111 Ms Stella Gray, *Submission No. 152*, p. 6.

112 iiNet, *Submission No. 108*, p. 11

113 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 11.

114 Australian Mobile Telecommunications Association – Communications Alliance, Submission No. 114,

2.140 In contrast, Telstra expressed significant reservations about the proposal for a tiered industry assistance model:

> Telstra believes these proposals run the risk of creating an uneven playing field, where the compliance burden would rest disproportionately with larger C/CSPs and the effectiveness of the overall regime is undermined by allowing criminals or terrorists to avoid interception arrangements by acquiring services from smaller C/CSPs.
>
> In relation to the interception cost sharing framework, the Discussion Paper indicates that a new tiered model may be introduced where larger C/CSPs are expected to have a comprehensive interception capability (presumably at a greater cost) while smaller C/CSPs may only be required to have a minimum level capability (presumably at a lower cost). While the Discussion Paper states that one of its aims is to maintain 'competitive neutrality' in the industry, it is hard to see how tiered compliance obligations are consistent with this aim. As such, Telstra does not support this proposal.[115]

2.141 In testimony before the Committee, Telstra expanded upon these concerns:

> Essentially what we are saying is that it should be a uniform application of obligations. Given the nature of their targets, law enforcement and national security schemes are only as strong as their weakest link. On an uneven playing field criminals and terrorists will inevitably locate their operations where security obligations are the lowest, leaving larger telecommunication operators to incur the costs of greater obligations for no offset in law enforcement or national security gain.[116]

2.142 Mr Mark Newton also opposed the proposal, submitting that a tiered model already applied by informal means:

> This proposal is unnecessary, on the grounds that we have it by fiat already. Current industry interception obligations are consultative, and the Attorney-General's Department doesn't bother to consult with providers that this proposal would envisage as 'tier 3.' I believe considering this proposal is a waste of time, and I don't support it.[117]

2.143 The Committee understands the proposal to be that all telecommunications providers would remain subject to an obligation to provide assistance to law enforcement and security agencies, but the manner in which telecommunications interception obligations would be discharged would vary according to the risk profile of the telecommunications provider. As such, the Committee is assured

---

p. 12.

115 Telstra, *Submission No. 189*, p. 9.

116 Mr James Shaw, *Transcript*, 27 September 2012, p. 2.

117 Mr Mark Newton, *Submission No. 87*, p. 9.

that lower tier telecommunications providers will still maintain interception capability.

2.144 The committee does not favour a tiered approach. However it acknowledges that there may be situations related to practicability and affordability where exceptions for particular industry players are justifiable. However it is for those who seek exemption from the uniform obligation to demonstrate why they should be excused.

Recommendation 15

The Committee recommends that the Government should develop the implementation model on the basis of a uniformity of obligations while acknowledging that the creation of exemptions on the basis of practicability and affordability may be justifiable in particular cases. However, in all such cases the burden should lie on the industry participants to demonstrate why they should receive these exemptions.

An offence for failure to assist in the decryption of communications

2.145 The AGD submission explains the rationale and scope of the decryption assistance proposal:

> Encryption is becoming widespread in information and communications technology. Criminals and terrorists are increasingly using encryption to avoid detection, investigation and prosecution causing difficulties for agencies to access clear, intelligible communications in their operations.
>
> Encryption can be difficult to manage. It may not always be the case that a person who uses or creates encryption is able to provide assistance with decryption. Often an applications provider, organisation or individual provides encryption services, rather than a carrier. Criminal organisations and terrorists can obtain these services or even create and use their own encryption solutions.
>
> Section 3LA of the *Crimes Act 1914* (the Crimes Act) sets out provisions concerning decryption regarding information obtained under search warrants; however this does not extend to communications intercepted pursuant to a warrant under the TIA Act.
>
> In summary, section 3LA of the Crimes Act allows a police officer to apply to a magistrate for a warrant to require a person to provide in accessible form (i.e. in decrypted form) data held on a computer or data storage device, where the computer or data storage device had been seized under a warrant. A warrant may be applied to the person under

> investigation, an owner of the device, an employee of the owner, a relevant contractor, a person who has used the device, or a systems administrator. There is a penalty of up to two years imprisonment for failing to comply with an order.
>
> A consistent approach to that contained in the Crimes Act would ensure that information lawfully accessed for national security or law enforcement purposes under the TIA Act was intelligible.[118]

2.146 The Committee received many submissions about the absence of clarity as to whom the proposed offences would apply to, and what type of decryption assistance is envisaged.

> End users, wholesale service providers, broadband retail service providers and content providers could all potentially play a role in the encryption of communications. Where the provider is based offshore then the matter of jurisdiction also needs to be considered.
>
> Any decryption requirement should also specify that the obligation is to make available, if it is available, the means for decryption, as opposed to the actual content/communications that is to be decrypted.
>
> There must not be a presumption that a person or organisation is capable of decrypting communications. The imposition of sanctions or penalties must be based on proof that the person or organisation is capable of assisting with the decryption of communications and there is evidence they have refused to do so.[119]

2.147 The AFP confirmed in testimony to the Committee that the decryption assistance sought by law enforcement agencies is limited to encryption applied by telecommunications providers:

> From our perspective, encryption is a terrific advancement for the Australian community. Because it helps protect people from those who would do them harm in scams and those sorts of things it is a very good thing. What we would be seeking as far as the uptake to the act goes is that, where we have a warrant to intercept particular information going to a particular service, that the service provider provide those encryption keys to us to allow us to undertake that interception under warrant—as I have said—rather than anything else. This is not about people's home encryption. This is about talking to service providers about their

118 Attorney-General's Department, *Submission No. 218*, pp. 6-7.

119 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 12. See also Mr James Sinnamon, *Submission No. 100*, p. 1; Privacy Victoria, *Submission No. 109*, p. 6; Mr Arved von Brasch, *Submission No. 126*, p. 3.

> providing those encryption keys under warrant for us to then intercept a particular device which has been duly authorised.[120]

2.148 The AFP provided a case study in support of the proposal:

> During an investigation into an online paedophile network, it was noted that targets deployed a multiplicity of encryption techniques. They sent messages using an encryption overlay; images were encrypted and 'hidden' within other images which were then sent via closed peer to peer networks which also used encryption. Advanced Encryption Standards applications were used on virtual machines (computers within computers). The combined effect meant persons of interest were able to browse the internet without leaving detectable forensic footprints for investigators.
>
> Additional members of this network identified and pursued in a related operation took the anti-forensic techniques further and used full disk encryption along with hidden volumes that were disguised using a technique that allowed for plausible deniability of the content, effectively circumventing both interception and search warrant legislation. Persons of interest identified in the investigation included a computer antivirus developer, and a computer networking trainer; their technical expertise was such that they were able to develop and customise their own encryption protocols rather than relying on off the shelf products.[121]

2.149 The Queensland Crime and Misconduct Commission expressed support for the proposal noting the current investigative challenge which encryption presents:

> The increased use of sophisticated encryption presents challenges to the CMC. Internet service providers (ISPs) as well as application service providers (ASPs) are increasingly providing end to end encryption. The fact that ASPs can be located anywhere in the world can make it extremely difficult to seek assistance in the decryption of content that may be vital in an investigation. TIA Act reform that envisages law enforcement agencies being able to request decryption assistance where possible from ISP's, Carriers and ASPs, would potentially allow for greater access to critical evidence.[122]

2.150 A range of submissions raised the prospect that an offence for failing to provide decryption assistance would undermine confidentiality requirements. The Electronic Frontiers Australia submission was indicative:

---

120 Commissioner Tony Negus, *Transcript*, 26 September 2012, p. 28.

121 Australian Federal Police, *Submission No. 163*, pp. 14-15.

122 Queensland Crime and Misconduct Commission, *Submission No. 147*, p. 7. See also Western Australia Corruption and Crime Commission, *Submission No. 156*, p. 10; Victoria Police, *Submission No. 200*, p. 15, Western Australia Police, *Submission No. 203*, p. 13.

> EFA is concerned about the possible creation of an offence for failing to assist in the decryption of communications for the following reasons:
>
> - it undermines the right of individuals to not cooperate with an investigation
> - it poses a threat to the independence of journalists and their sources, particularly in circumstances involving whistle-blowing activity related to cases of official corruption
> - it could undermine the principles of doctor-patient and lawyer-client confidentiality and other trusted relationships
> - there are foreseeable and entirely legitimate circumstances in which decryption of data is not possible, such as where a password has been forgotten and is unrecoverable.[123]

2.151 The Human Rights Law Centre submitted that decryption assistance could impose an obligation on suspects to provide a 'level of assistance to investigators [that] runs counter to the right to remain silent.'[124]

2.152 Mr Ian Quick objected to the proposal on a number of practical and theoretical grounds:

> On the practical front, what would an agency do if someone said
>
> - 'I can't remember the password'
> - 'I've deleted whatever the password was that was used for that period, so cannot assist.'
> - 'I didn't know it was encrypted, so have no idea what you are talking about.'
> - 'It's not encrypted, it's just random junk (for whatever reason..)'
> - 'The password I gave you doesn't work? The file/message must be corrupted,
> - I can't help you.'
>
> In addition, many communication protocols regularly used on the internet have session keys used for encryption, which are not recoverable by the end user.
>
> What would the agency do? All the responses above might be legitimate, I have certainly experienced every one of them! How would you distinguish between someone who was truthfully saying it and someone who was lying? Surely it would be against the presumption of innocence to fine/jail people who failed to assist unless it could be proven that they could assist – and how could this be done? How would it be legislated?[125]

123 Electronic Frontiers Australia, *Submission No. 121*, p. 15

124 Human Rights Law Centre, *Submission No. 140*, p. 11. See also, Mr Breheny, *Transcript*, 5 September 2012, p. 45; Mr Bernard Keane, *Submission No. 117*, p. 12.

125 Mr Ian Quick, *Submission No. 95*, p. 13.

2.153 The Law Council of Australia gave in principle support for assisting agencies access communications once authorised, but queried whether an offence was the appropriate mechanism:

> However, the Law Council also appreciates the need to ensure that officers who have been authorised to access communications can do so in an effective, meaningful way.
>
> To this end, the Law Council does not oppose mechanisms to assist agencies to reconstruct or decrypt the content of communications to which access has been authorised.
>
> It notes for example, that the Telecommunications Act already obliges carriers and carrier service providers to provide such help to agencies as is 'reasonably necessary' for enforcing the criminal law and laws imposing pecuniary penalties, protecting public revenue and safeguarding national security.
>
> However, it is not clear on the basis of the information provided in the Discussion Paper that the introduction of a criminal offence, presumably aimed at participants in the telecommunications industry such as carriers and carriage service providers, would be an effective or appropriate response, particularly when other non-punitive efforts may to be available to enhance cooperation between the agencies and the telecommunication industry.
>
> Before introducing criminal liability for failing to assist in the decryption of communications, the Law Council suggests that the PJCIS requests that information be provided by the Attorney-General's Department that explains whether the proposed offence adheres to the principles contained in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*.[126]

2.154 The Committee notes that, like the proposal for data retention, much of the discussion of the proposal for decryption assistance was confused by the lack of clarity on what is being proposed.

2.155 The Committee understands the proposal is for an offence to apply where a telecommunications provider does not provide assistance to decrypt communications where those communications have been encrypted by that telecommunications provider. This will of course only arise in circumstances where the relevant national security agency has established grounds where it is necessary to intercept and decrypt the communication. That being the understanding, many of the concerns raised by submitters about individuals being subject to the offence, or being forced to provide passwords, do not apply.

126 Law Council of Australia, *Submission No. 96*, p. 36.

2.156 The Committee notes encryption can impede access to telecommunications interception where access to the content of communications has been lawfully authorised.

2.157 The Committee acknowledges, however, that there remains a lack of specificity regarding the scope of the offence and the circumstances in which it may apply. In this context, the Committee appreciates the guidance provided by the Law Council of Australia in referring to the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*.

Recommendation 16

The Committee recommends that, should the Government decide to develop an offence for failure to assist in decrypting communications, the offence be developed in consultation with the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. It is important that any such offence be expressed with sufficient specificity so that telecommunications providers are left with a clear understanding of their obligations.

Institute industry response timelines

2.158 The Western Australia Police expressed support for the imposition of industry timelines for assistance sought from telecommunications providers:

> It is important that telecommunication carriers are capable of dealing with urgent requests for communications data. This is particularly relevant when dealing with stored communications data. It is the practice of some carriers to purge such data after a short period of time. To ensure that evidence is not lost, carriers must have the capability of immediately responding to requests from law enforcement agencies to preserve the data, or alternatively they must have a reasonable ability to store data to until the completion of a police investigation.[127]

2.159 Optus expressed concern if the timeliness proposal was raised as more than a minimum standard:

> Optus does not support mandated response times for warrants, unless it is calibrated as a backstop for extremely poor responsiveness. If the objective is to achieve an overall improvement in timeliness, then the

127 Western Australia Police, *Submission No. 203*, p. 13. See also: Western Australia Corruption and Crime Commission, *Submission No. 156*, pp. 10-11.

> focus should be on end-to-end process opportunities, taking into account both the agency activities and the carrier activities. The adoption of more effective and complete B2B electronic transaction processes for warrants by both agencies and carriers could drive substantial improvements in timeliness.[128]

2.160 In relation to requirements for timeliness however, the Australian Mobile Telecommunications Association and Communications Alliance considered the current regime enables the law enforcement and national security agencies to negotiate service levels for the supply of reasonably necessary assistance.[129]

2.161 Similarly, iiNet did not support the proposal, noting an absence of justification:

> iiNet submits that imposing specific industry timeframes is unnecessary. iiNet notes that there is no suggestion in the Discussion Paper that industry tardiness is in any way a cause of any of problems for law enforcement agencies.[130]

2.162 Telstra indicated a significant resource implication from the proposal:

> Telstra submits that for Government to mandate 'response timelines' would also require Government to spend significant funds to support the introduction of a fully automated request management system (as discussed in 8a) for use by LENSAs and C/CSPs otherwise the LENSAs would not obtain the benefits intended from this proposal.[131]

2.163 The Committee notes the need to ensure that telecommunications providers are able to provide timely assistance to law enforcement and national security investigations. The evidence presented to the Committee, however, was sparse on the question of whether or not such assistance is presently provided in a timely manner.

2.164 The Committee acknowledges, however, that clearly expressed obligations would enable telecommunications providers to better assist the investigative agencies.

---

128 Optus, *Submission No. 206*, p. 2.

129 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 13.

130 iiNet, *Submission No. 108,* p. 12.

131 Telstra, *Submission No. 189*, p. 10.

Recommendation 17

The Committee recommends that, if the Government decides to develop timelines for telecommunications industry assistance for law enforcement and national security agencies, the timelines should be developed in consultation with the investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority.

The Committee further recommends that, if the Government decides to develop mandatory timelines, the cost to the telecommunications industry must be considered.

Revision of the interception regime

2.165 Submissions and testimony provided to the Committee, particularly from interception agencies, indicate a desire for a comprehensive revision of the TIA Act. For example, the Western Australia Police submission states:

> WA Police supports the suggested reform of the TIA Act in its entirety, for ease of understanding and in order to remove duplication. Further, there is a need to update the content of the TIA Act to ensure that the provisions are practical and responsive.[132]

2.166 In its submission, the AGD supports the proposal for comprehesive reform, stating:

> The magnitude of current and anticipated change to the telecommunications landscape means it is now timely to consider whether the privacy needs of Australians and the investigative needs of law enforcement and national security agencies are best served through continuous ad-hoc change or whether the time is right to put in place a new interception framework that squarely focuses on the contemporary communications environment. The Department considers that holistic reform would establish a new foundation for the interception regime that enables users and participants, as well as the broader Australian community to understand their powers, rights and obligations.[133]

132 Western Australia Police, *Submission No. 203*, p. 9.

133 Attorney-General's Department, *Submission No. 218*, pp. 2-3

2.167 The Committee received extensive evidence from interception agencies, privacy advocates and legal practitioners about the complexity of the TIA Act. Indeed, the Committee's consideration of the statutory framework supports the conclusion that it is so complex as to be opaque in a number of areas. That this is the case in legislation which strives to protect the privacy of communications and enabling legitimate investigative activities is of concern.

2.168 The Committee acknowledges, however, the risks associated with comprehensive revision of legislation and that a cautious approach is necessary. Privacy Victoria noted in-principle support for revision to achieve technological neutrality, but cautioned:

> However, when revising these laws, the goal should not be to lower protections contained within, but rather to standardise and enhance existing protections irrespective of the method of communication (that is, to make the laws technologically neutral).[134]

2.169 The Committee did not have the advantage of receiving draft legislation to review. That being the case, there is an inherent difficulty in recommending comprehensive revision of the TIA Act in the absence of draft proposals.

2.170 The Committee acknowledges, however, that the TIA Act is complex. It could be improved significantly by providing clear direction on the protections afforded to telecommunications users, and the scope of the powers provided to agencies able to undertake telecommunications interception and access to stored communications and telecommunications data.

2.171 Implementing the recommendations of this report necessitates a significant revision of the interception regime. The Committee therefore supports comprehensive revision of the TIA Act.

134 Privacy Victoria, *Submission No. 109*, p. 2

Recommendation 18

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* (TIA Act) be comprehensively revised with the objective of designing an interception regime which is underpinned by the following:

- **clear protection for the privacy of communications;**
- **provisions which are technology neutral;**
- **maintenance of investigative capabilities, supported by provisions for appropriate use of intercepted information for lawful purposes;**
- **clearly articulated and enforceable industry obligations; and**
- **robust oversight and accountability which supports administrative efficiency.**

The Committee further recommends that the revision of the TIA Act be undertaken in consultation with interested stakeholders, including privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies.

The Committee also recommends that a revised TIA Act should be released as an exposure draft for public consultation. In addition, the Government should expressly seek the views of key agencies, including the:

- **Independent National Security Legislation Monitor;**
- **Australian Information Commissioner;**
- **ombudsmen and the Inspector-General of Intelligence and Security.**

In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.