Chapter 3

Warranted access to telecommunication content

3.1 The *Telecommunications (Interception and Access) Act 1979* (TIA Act) provides a legislative framework that criminalises the interception and accessing of telecommunications. However, the Act prescribes exceptions that enable law enforcement, anti-corruption and national security agencies to apply for warrants to intercept communications when investigating serious crimes and threats to national security. The warrant regime provides these agencies with lawful access to telecommunications content.

3.2 This chapter provides an overview of the existing warrant framework within the TIA Act and then discusses opportunities for legislative reform. The overview provides an insight into the complexity of the current legislation.

3.3 In examining the warranted access regime to telecommunications content, the committee was informed by the 2013 report of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) which recommended that the proportionality test within the TIA Act be revised and consideration be given to implementing a consistent proportionality test across interception and access to telecommunications content. The committee was also informed by the 2015 report of the PJCIS into mandatory data retention that re-considered the issue of proportionality in context of necessity, efficacy and the current risk environment.[1]

An overview of the warrant regime

3.4 Chapters 2 and 3 of the TIA Act[2] provide for warranted access to telecommunications, including both communications passing across telecommunications services (that is, the interception of live communications), and stored telecommunications content.[3]

3.5 The Attorney-General's Department (the department) provided the following description of the four existing warrant regimes that enable law enforcement and anti-corruption agencies to lawfully access the content of communications:

[1] PJCIS data retention report, paragraph 2.102, p. 37.

[2] The TIA Act is comprised of five chapters.

[3] The process which the Australian Security and Intelligence Organisation (ASIO) is required to follow for warrants, differs to those for anti-corruption agencies and law enforcement agencies and has not been specifically addressed in the body of the report. The sections relevant to ASIO are sections 9, 9A and section 109 of the TIA Act. By way of example, where ASIO has applied to the Attorney-General for a warrant under section 9 of the Act, the Attorney-General may issue a warrant where satisfied that the telecommunication service is being used, or is likely to be used in 'activities prejudicial to security' and interception will, or is likely to, assist the organisation in carry out its functions. 'Activities prejudicial to security' is defined in section 4 of the *Australian Security Intelligence Organisation Act 1979*.

> The TIA Act contains four warrant regimes for lawful access to the content of communications by law enforcement and anti-corruption agencies. Three of these warrants relate to access to 'live' communications, and the fourth relates to access to 'stored' communications held by carriers.
>
> The distinction between access to live and stored communications currently embodied in the TIA Act is based on an assumption that stored communications were generally more 'considered' and so less privacy sensitive.[4]

3.6 In addition, the Act provides for warrants to be issued for specific purposes, such as locating missing persons or locating a caller in an emergency.

Telecommunications service warrants and named person warrants

3.7 The provisions within Chapter 2 of the TIA Act enable 'agencies' to apply for telecommunications service warrants and named person warrants to an eligible judge or nominated member of the Administrative Appeals Tribunal (AAT). The Act prescribes that the judge or nominated member of the AAT may issue a warrant in the circumstances where they are satisfied that the information likely to be obtained under the warrant would be likely to assist in the investigation of a 'serious offence' and they have had regard to a number of factors to ensure that the issuing of a warrant is proportionate in the circumstances.[5] This is referred to as a proportionality test.

3.8 For the purposes of Chapter 2 of the TIA Act, 'agencies' is defined as 'interception agencies' which is further defined as the Australian Federal Police (AFP), the Australian Crime Commission (ACC) or the Australian Commission for Law Enforcement Integrity (ACLEI); or an eligible authority of a state in relation to which a ministerial declaration under section 34 is in force. Section 34 of the TIA Act enables the Minister, by legislative instrument, at the request of the Premier of a State, to declare an 'eligible authority' of that State to be an 'agency' for the purposes of the Act. The Act defines an 'eligible authority' in relation to a state to mean:

- in any case—the police force of that state; or
- in the case of New South Wales—the Crime Commission, the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the Police Integrity Commission or the Inspector of the Police Integrity Commission; or
- in the case of Victoria—the Independent Broad-based Anti-Corruption Commission (IBAC) or the Victorian Inspectorate; or
- in the case of Queensland—the Crime and Misconduct Commission; or
- in the case of Western Australia—the Corruption and Crime Commission or the Parliamentary Inspector of the Corruption and Crime Commission; or

[4] Attorney-General's Department, *Submission 26*, p. 17.

[5] See sections 46 and 46A of the TIA Act which set out the factors to which the Judge or AAT member must have regard when considering an application for a telecommunications service interception warrant or a named person warrant.

- in the case of South Australia—the Independent Commissioner Against Corruption.

3.9 'Serious offence' is defined in section 5D of the TIA Act. The definition is complex but includes, among other things, murder, kidnapping, bribery, market misconduct and other offences that are punishable by imprisonment for life or for a period, or maximum period, of at least seven years.

Stored telecommunications warrants

3.10 In certain circumstances, 'enforcement agencies' (defined below) can require that a carrier preserve all stored communications the carrier holds that relate to the person or telecommunications service specified in a notice.[6] The communications stored may then be accessed, by warrant, in prescribed circumstances.[7] Like telecommunications service warrants, a proportionality test is also applied. The proportionality test applied in this circumstance involves 'serious contravention'.

3.11 Where an 'enforcement agency' has applied to an 'issuing authority' (defined below) for a stored telecommunications warrant, the TIA Act provides that the 'issuing authority' may issue the warrant if satisfied that the information likely to be obtained under the warrant would be likely to assist in the investigation of a 'serious contravention' and the 'issuing authority' has had regard to a number of matters to ensure that the issuing of a warrant is proportionate in the circumstances.[8]

3.12 'Enforcement agency' is defined in section 5 of the TIA Act. The definition includes: the AFP, a police force of a state, anti-corruption bodies, the ACLEI, the ACC, authorities prescribed by legislation, and, any body whose functions include: (i) administering a law imposing a pecuniary penalty; or (ii) administering a law relating to the protection of the public revenue.

3.13 'Issuing authority' is defined in section 5 of the Act as 'a person in respect of whom an appointment is in force under section 6DB'.[9] Certain judges, magistrates and AAT members who are also enrolled as legal practitioners may be appointed by the Minister to be an 'issuing authority'.[10]

3.14 'Serious contravention' is defined in section 5E of the TIA Act. Like the definition of 'serious offence' in section 5D of the Act, the definition of 'serious contravention' in section 5E is complex. It includes a Commonwealth, state or territory offence punishable by imprisonment for a period, or a maximum period, of at least three years. The definition also includes offences punishable by a maximum fine

[6] The legislative framework governing stored telecommunications warrants is set out in Chapter 3 of the TIA Act.

[7] See Chapter 3 of the TIA Act.

[8] Subsection 116(2) of the TIA Act sets out the matters to which the issuing authority must have regard when considering an application for a stored communications warrant.

[9] This definition presents particular issues in relation to access to telecommunications data which are examined in Part II of this report.

[10] Sections 5, 5E and 6DB, TIA Act.

of at least 180 penalty units[11] or a contravention of the law which would make an individual liable to pay a pecuniary penalty of the same magnitude.

Removing legislative duplication in the warrant regime

3.15 Throughout this inquiry the committee received evidence regarding the complexity of the existing legislative framework that governs warranted access to telecommunications content.[12] Stakeholders consistently impressed upon the committee the need to remove legislative duplication from the warrant framework. Many proposed the introduction of a single warrant regime that authorised interception of content, whether live or stored, on the basis of prescribed attributes. This is referred to as 'attribute-based interception'. Proponents of this approach argued that it would reduce complexity by removing the distinction between a 'serious offence' and a 'serious contravention' while also providing a single clear proportionality test.[13]

3.16 Submitters identified an administrative burden associated with the complex duplication within the existing TIA Act. The then Director-General of Security explained:

> [I]n order to look at a particular individual we may need to take out three or four different warrants, each of which requires a considered three- or four-page argument, and yet the argument is actually the same in all of the warrants. So to be able to combine a number of warranted activities together…is one such example. The ability to intercept according to a number of different selectors, rather than just the name of a person and a telephone number, for example, to be able to intercept on the basis of other attributes—call areas, time or whatever—would be a great help. It does not in any way change the level of intrusiveness but it simply makes the bureaucratic processes a lot simpler.[14]

3.17 ASIO noted however, that there would be instances where legislative duplication would remain both necessary and appropriate:

> Over time, the many amendments to the TIA Act have resulted in duplication and complexity making the Act difficult to understand and apply. Conversely, there is intentional duplication for provisions that apply specifically to ASIO with separate provisions for enforcement agencies. For example, voluntary disclosure provisions for ASIO are covered under

[11] One penalty unit is currently $170.

[12] Among others, the following organisations cited support for removal of legislative duplication: Victoria Police, *Submission 6*, p. 2; Western Australian Corruption and Crime Commission, *Submission 14*, p. 16; Northern Territory Police, *Submission 21*, p. 8; and New South Wales Government, *Submission 30*, p. 13.

[13] These same matters were canvassed by the PJCIS throughout its inquiry which reported in June 2013 (see that committee's recommendations 6, 7 and 10) and are discussed further at paragraphs 3.27 and 3.28 of this chapter.

[14] Mr David Irvine, Director-General of Security, Australian Security Intelligence Organisation (ASIO), *Committee Hansard*, 21 July 2014, p. 7.

> section 174 whereas section 177 relate[s] to enforcement agencies. ASIO supports the recommendation to remove legislative duplication but notes it should not be applied in instances where there is a necessary distinction between ASIO's security intelligence role and law enforcement agencies.[15]

3.18 The Australian Federal Police (AFP) stated that in its view, '[r]emoving duplicative processes and complexity within the TIA Act [would] simplify the processes for agencies and may assist in achieving transparency by removing legislative intricacy'.[16] The Australian Mobile Telecommunications Association (AMTA) and the Communications Alliance similarly supported removing legislative duplication; these organisations added that legislative duplication between the TIA Act and the *Telecommunications Act 1997* (Telecommunications Act) should also be considered.[17]

3.19 Although many submitters were strongly supportive of a single warrant regime, the Law Council of Australia (Law Council) cautioned that it would be important not to introduce such a regime at the expense of privacy safeguards:

> The Law Council supports the removal of legislative duplication but not where this involves a single warrant regime which would make it difficult for issuing authorities to adequately assess the privacy impacts of the powers under the warrant. Given the particularly intrusive nature of telecommunications interception, legislative clarity must not be achieved to the detriment of privacy principles.[18]

A single attribute-based interception regime

3.20 The department explained that under the existing provisions of the TIA Act, warrants issued may only authorise the interception of 'services' or 'devices'—such as a particular internet connection or telephone:

> The service or device identifiers are the technical means that the telecommunications industry uses to identify the communications for retrieval under a warrant. This approach is technologically-specific and reflects historic assumptions about how telecommunications operate. The diversification of the telecommunications industry, changing communications habits and changes to the technical operation of modern telecommunications networks mean that new ways of identifying communications are both available and required.[19]

3.21 The department stated that in its view '[w]ithout reform, technological change will make the current, service and device-based provisions obsolete'.[20] The department

[15] ASIO, *Submission 27*, p. 34.

[16] Australian Federal Police, *Submission 25*, Attachment E, p. 5.

[17] Australian Mobile Telecommunications Association and Communications Alliance, *Submission 16*, pp 7–8.

[18] Law Council of Australia, *Submission 34*, pp 39–40.

[19] Attorney-General's Department, *Submission 26*, p. 17.

[20] Attorney-General's Department, *Submission 26*, p. 17.

recommended the single attribute-based warrant regime as a more targeted and technologically-neutral approach:

> [T]he reality is that this Act was very cleverly drafted in 1979 in that it was technologically neutral and it has been able to capture all communications as they have come along, without any need to consider the implications of that technology. The reality now is that people communicate with very smart phones…and they do allow you to communicate in many, many ways with one device. The Act really is just saying that law enforcement can intercept that device without any approach that allows you to target the kind of information that you want.
>
> What the Act does not do at the moment is have any real way to define what kind of information should be collected by law enforcement for them to investigate crimes. What the Act currently says is you can collect evidence; however, you must do it in a very broad, crude way.[21]

3.22 The department explained that it was advocating for a change in the legislation to a single attribute-based warrant regime as such a regime would:

- better protect the privacy of communications 'because law enforcement and national security agencies [would] have to determine the kind of communications they want to collect'; and
- allow telecommunications providers 'to target a stream of traffic rather than volumes of traffic'.[22]

3.23 ASIO echoed these views. According to ASIO, the TIA Act, as currently written, 'limits the technical means by which agencies can conduct interception by requiring interception be based on either a "service" identifier (for example, a telephone number or email address) or a piece of "equipment" (for example, a mobile telephone handset)'.[23] ASIO advocated the 'decoupling' of the techniques for interception from the authorisation to intercept and expressed its support for attribute-based interception:

> "Attributes" are specific identifying characteristics that can be used in combination to identify unique communications of interest to ASIO. Attribute-based interception encompasses service-based or equipment-based interception. It also allows ASIO to target specific attributes to collect communications of interest more effectively and less intrusively.[24]

3.24 ASIO provided some examples of attributes that could be used:

> - …some individual attributes that could be combined to enable better interception targeting could include:

[21] Ms Katherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Proof Committee Hansard*, 22 April 2014, p. 3.

[22] Ms Katherine Smith, Attorney-General's Department, *Committee Hansard*, 22 April 2014, p. 3.

[23] ASIO, *Submission 27*, p. 33.

[24] ASIO, *Submission 27*, p. 33.

- the source and/or destination of the communication;
- the type of communication (for example, a video call, email, SMS);
- the equipment being used to convey the communication (for example mobile telephone handset, cell tower);
- any identifier being used in connection with the communication (such as a number or username);
- a time period in which a communication is made or received; or
- the location of the person making or receiving the communication.

3.25 The selection of a combination of attributes in each particular case would involve a number of considerations, including the extent to which:

- the telecommunications provider had the ability to intercept the chosen attributes;
- attributes (singly or in combination) were sufficiently precise to give a high degree of certainty communications of interest are accessed; and
- certain components of a communication could be excluded on the basis they were likely to be irrelevant.[25]

3.26 In ASIO's view the approach of 'attribute-based interception':

> …would allow agencies to filter and limit the communications they intercept more efficiently, helping to minimise the collection of extraneous information. With this more specific method of targeting the telecommunications of interest, the more certain we can be that we are excluding from incidental interception the communications of persons who are not of interest and whose privacy should be protected.[26]

3.27 In its 2013 report, the PJCIS observed that advancements in telecommunications technology were diminishing the effectiveness of the current interception framework. As a result, the PJCIS recommended that the interception of communications should be conducted on the basis of specific attributes of communications as a means of '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'.[27]

3.28 Submitters to this inquiry cited the PJCIS's recommendation of a single warrant regime and suggested that the introduction of such a regime would be a means by which telecommunications interception legislation could be simplified and also

[25] ASIO, *Submission 27*, p. 33.

[26] ASIO, *Submission 27*, p. 33.

[27] PJCIS, Report of the Inquiry into Potential Reforms of Australia's National Security Legislation, June 2013, p. 34.

respond to advancements in technology. The ACC and AFP also expressed support for a single attribute-based interception regime.[28]

How would it work?

3.29 The department explained how it anticipated 'attribute-based' interception would apply in practice. A warrant would still need to be issued to authorise access to a particular person's communications but, according to the department, that 'attribute-based' warrant:

> …would describe the communications that the service provider is to access and provide to the agency by using a combination of technical features or 'attributes'—rather than just a service or device identifier. Those attributes could include a specific account, a time of day, a geographic location or a technical feature of the communication.[29]

3.30 The department explained that, in its view, attribute-based interception would enable warrants to be more targeted and would also minimise the lawful collection of irrelevant communications.

Concerns raised in relation to attribute-based interception

3.31 Although there was wide-spread support for the introduction of an attribute-based interception warrant regime throughout the law enforcement community, some concern was expressed by other stakeholders.

3.32 The Law Council advised that its reservations in relation to attribute-based interception are based on the view that 'attribute-based' has not been sufficiently defined to allow the 'true privacy implications' associated with such a model to be assessed.[30]

3.33 In raising its objections, the Law Council noted the challenges that 'existing and emerging telecommunications technologies pose for agencies attempting to accurately identify the communications they intend to intercept or access',[31] and went on to express general support for:

> …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 this 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.[32]

[28] See: ACC, *Submission 23*, Attachment A, p. [3] and AFP, *Submission 25*, Attachment E, p. 4.

[29] Attorney-General's Department, *Submission 26*, p. 18.

[30] Law Council of Australia, *Submission 34*, pp 33–34.

[31] Law Council of Australia, *Submission 34*, pp 33–34.

[32] Law Council of Australia, *Submission 34*, pp 33–34. This view was shared by AMTA and the Communications Alliance. See: *Submission 16*, p. 6.

3.34 The department explained to the committee that a single attribute-based warrant would enable more targeted interception and, therefore, provide a higher level of privacy protection. To demonstrate this, the department noted how the current framework provides for a law enforcement agency to intercept a device without any approach to targeting the kind of information wanted:

> [For example] [a]t the moment, a service warrant would allow you to collect against a particular service. If it is Joe Bloggs's smart phone, that actually is the service, and everything that sits on that smart phone—every bit of content, whether it be Candy Crush, Skype or their email—that service is all of that, and the warrant does not have the specificity at the moment to say, "Actually, we don't want their livestreaming of the cricket; we just want the particular communication".
>
> …
>
> The problem at the moment is that the warrant is quite broad in its approach, and what we want to do is have much better specificity. It may be that they will collect the voice, the email and the livestream of the cricket, but we want to be able to identify those as attributes of the whole communication channel rather than just saying, "Give it all to us, and we'll decipher it later".[33]

3.35 In expressing support for the introduction of a single attribute-based warrant regime both ASIO and the ACC acknowledged the need to ensure the maintenance of 'the proportionality thresholds and accountability requirements…to deliver public confidence and assurance regarding the use of these powers'[34] in any new regime.

Senator Scott Ludlam
Inquiry Chair

[33] Ms Katherine Smith, Attorney-General's Department, *Committee Hansard*, 22 April 2014, p. 3.

[34] ASIO, *Submission 27*, p. 35. See also: ACC, *Submission 23,* Attachment A, p. [6].