CHAPTER 4

B-PARTY INTERCEPTION

Introduction

4.1 One of the most contentious aspects of the Bill is contained in Schedule 2 which deals with the so-called 'B-party' warrants. Briefly, in the words of the Explanatory Memorandum, the provisions 'enable interception of communications of a person known to communicate with the person of interest'.[1]

4.2 B-party warrants are issued by the Attorney-General in the case of an application by the Director-General of ASIO, or by an 'eligible judge' or member of the AAT in the case of an application by a law enforcement agency.

4.3 The warrant may only be issued for offences which attract a maximum penalty of seven years' gaol. Further, they will only be issued to an interception agency which has satisfied the issuing authority:

- that it has exhausted all other methods of identifying a telecommunications service used by a person of interest; or that it is not possible to intercept the communications of the person of interest; and
- that the person being intercepted will likely be contacted by the person of interest on the service being intercepted.

4.4 When issuing the warrant, the issuing authority must also have regard to the following:

- the extent to which the proposed interception interferes with the privacy of any person;
- the gravity of the offences being investigated;
- the extent to which the information obtained under the warrant will assist the investigation;
- the extent to which alternative methods of investigation have been used or are available to the agency; and
- the extent to which these alternative methods would be useful to or would prejudice the investigation.

---

1 Explanatory Memorandum to the Telecommunications (Interception) Amendment Bill 2006, p. 1.

4.5 Once issued, the warrants are available for 45 days for law enforcement agencies and 30 days for ASIO. This is half the time provided for the execution of existing telecommunications interception warrants.

Rationale for B-party interception warrants

4.6 The necessity for this type of interception warrant was explained by the Attorney-General in his Second Reading speech. The Attorney General said:

> This amendment will assist interception agencies to counter measures adopted by persons of interest to evade telecommunications interception, such as adopting multiple telecommunications services. The ability, as a last resort, to intercept the communications of an associate of a person of interest will ensure that the utility of interception is not undermined by evasive techniques adopted by suspects.

4.7 The provisions had their genesis in the *Report of the Review of the Regulation of Access to Communications* ('The Blunn Report').2 In Part 12 of that report, Blunn observed that the current *Telecommunications Interception Act 1979* does not authorise the use of B-Party intercepts.[3]

4.8 In his exploration of the issue, Blunn observed that the security and law enforcement agencies argue that there is a need for B party interception, and noted its usefulness in appropriate circumstances. However he cautioned the need for 'appropriate controls, and the need to acknowledge and deal with the significant privacy implications.'4 Accordingly, his Recommendation 12 states:

> I recommend that the Interception Act be amended to make it clear that B-Party services may be intercepted in limited and controlled circumstances.[5]

4.9 Officers of the Attorney-General's Department gave more detailed evidence of this issue to the Committee. Mr Geoff McDonald Assistant Secretary of the Security Law Branch explained that:

> … we are facing a practical problem which some law enforcement agencies are very concerned about. It is due to people becoming more savvy about these matters. ... People are savvy enough now, if they are involved in the criminal side of things, to use the technology.[6]

4.10 From a policing point of view, the Deputy Commissioner of the Australian Federal Police observed that the proposals would clarify the position in relation to

---

2 Blunn, A S, AGPS, August 2005

3 Blunn, p. 76.

4 Blunn, p. 76.

5 Blunn, p. 77.

6 *Committee Hansard*, 15 March 2006, p. 52.

B-party warrants and provide an 'important investigative tool' for the AFP.[7] He explained:

> Where we have … multiple phones changing and SIM cards changing, it is often hard for law enforcement to identify the suspect's telecommunications service. Intercepting a close or known associate, somebody who we have to satisfy in accordance with the criteria you have just heard about and in the context of an affidavit before a magistrate as to what the nexus between the two is and why we believe that may produce the communications service of the suspect, is necessary.[8]

4.11 Assistant Commissioner Lawler gave several examples of situations in which the amendments would assist police. He proffered the following hypothetical case:

> With suspected purchases of explosive chemicals that are outside the norm, a particular chemical company has come forward and advised us that a particular person will call in. He does not know who the person is. He might have given a name; it could be false, but they will ring in to the chemical company and advise delivery and other sorts of details et cetera. The B-party warrant in that situation, given the current legislation, says that the person must be involved in the offence. [9]

4.12 In another example, he explained that:

> … when we use undercover operatives or cooperating informants it is often necessary to have these people call particular individuals to gather evidence as to the ongoing commission of offences or offences that may have been perpetrated. That is one of the tactical techniques but as it currently stands under the law one cannot get a telephone intercept because one is required to establish that the service belongs to a person who is involved.[10]

4.13 The Committee also notes that an important element of the current proposal is the clarification of the existing law on B-party warrants, which appears to give partial approval for their use.

4.14 As Mr Blunn commented, this matter was explored by the Federal Court in *John Flanagan and Ors v the Commissioner of the AFP and ors FCA (1995)* in which the court upheld the validity of B-party interception under the existing interception warrant regime but 'did not provide any useful analysis of the rationale'.[11] Assistant Commissioner Lawler indicated that the case created ambiguity and uncertainty over lawfulness of B-party interception under the Section 45 and 45A provisions:[12]

---

7 *Committee Hansard*, 15 March 2006, p. 32.

8 *Committee Hansard*, 15 March 2006, p. 44.

9 *Committee Hansard*, 15 March 2006, p. 46.

10 *Committee Hansard*, 15 March 2006, p.

11 Blunn, p. 76.

12 *Committee Hansard*, 15 March 2006, p. 45.

> … there are examples where some of the circumstances surrounding the current legislative provisions, namely, 45 and 45A, actually capture the spirit of B-party warrants.[13]

4.15 Mr Geoff McDonald of the Attorney-General's Department expanded on this:

> The interesting thing about it is that it can so easily be restricted to the facts of a particular case and distinguished, but from a policy perspective we certainly need to have a decent codified position on this rather than trying to rely on peculiar facts of a particular case.[14]

4.16 The Committee notes that in his submission to the Committee, the Hon Duncan Kerr SC MP refutes the existence of any common-law right for third party interception, and states that the only lawful basis for the interception of a telephone service is through the *Telephone (Interception) Act 1979*.[15]

4.17 The Committee further notes the statement of Mr Carnell, Inspector General of Intelligence and Security:

> the nature of B-Party interception warrants inherently involves a potential for greater privacy intrusion for persons who may not be involved in activities of legitimate concern under the ASIO Act. As a result, particular attention will be given to the additional legislative tests for this type of warrant, as well as checking that the duration of 90 days is adhered to.[16]

The counter view: B-party interception not necessary

4.18 Other submissions rejected outright these justifications for the creation of the warrants, arguing that they are an unwarranted invasion of privacy and that the necessary information can be gained by existing means.

4.19 Mr Cameron Murphy of the NSW Council for Civil Liberties, while acknowledging that the purpose of the principal Act is to protect the privacy of people using communications devices, remained concerned that this amendment represents 'a massive expansion of the invasion into people's privacy who use telecommunications devices' and maintained that there is no real justification for it:

> We can accept that, if someone is a suspect in a criminal investigation, it is a matter of balancing the interests of the public in ensuring that that suspected offence is investigated and that the person is prosecuted and dealt with under the law. In this amendment, we are dealing with something that goes much further than that. We are talking about innocent B-parties, people who are not themselves suspected of any offence … B-party warrants … shift[s] the focus of the investigation from someone who is a

13 *Committee Hansard*, 15 March 2006, p. 44.

14 Ibid.

15 *Submission* 1, p. 4.

16 Submission 9, pp 2-3.

> suspect to an investigation surrounding the innocent B-party on the off-chance that a suspect might contact them and there might be useful information gleaned that way…. [17]

4.20 Similarly, the Law Council of Australia observed that:

> Schedule 2 of the Bill if enacted allows certain law enforcement agencies and ASIO to intercept telecommunications of a person who has no knowledge or involvement in a crime, but who may be in contact with someone who does. In other words, people suspected of nothing will be under surveillance. … This is the first time ever in Australia's history that law enforcement agencies will be given power to intercept telecommunications of people who are not suspects, who are innocent people.[18]

4.21 In their submission to the inquiry, the Gilbert and Tobin Centre of Public Law states:

> We believe, however, that the Bill abrogates the right to privacy substantially more than is necessary to achieve the Bill's security purposes. It is important that legislation does not abrogate rights more than is necessary and incidental to achieving the purpose of the legislation.
>
> Where legislation does disproportionately abrogate rights, it may have adverse, unintended effects.[19]

4.22 Electronic Frontiers Australia was also concerned about the provisions, the Executive Director saying that the organisation is 'completely opposed' to the B-party warrant provisions. Similarly, the Australian Privacy Foundation urges the provisions be excised from the Bill until they can be given further consideration.[20]

4.23 The Law Council of Australia argued that the proposals breach Article 17 of the International Covenant on Civil and Political Rights and described the proposals as an 'arbitrary' invasion of privacy.[21]

4.24 The NSW Council for Civil Liberties agreed and further said that the provisions are also unjustified on practical grounds. Mr Murphy told the Committee:

---

17 Ibid.

18 *Submission* 17, p. 6.

19 *Submission* 2, p. 1.

20 *Submission* 4, pp 8-9.

21 *Committee Hansard,* 15 March 2006, p. 2, Submission 17, p. 6.

Article 17 ICCPR states:

1. 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.
2. Everyone has the right to the protection of the law against such interference or attacks.

> It appears to us that any of the evidence sought by law enforcement agencies could be obtained through an ordinary service warrant or a named person warrant. We have not yet seen a single example that stands up to even basic scrutiny about why a B-party warrant might be needed in order to obtain evidence about the suspect.[22]

Committee view

4.25 The Committee accepts that rapidly developing technology, and the increasing tactical sophistication of the targets of investigations, requires new approaches by law enforcement agencies if they are to remain effective. The current uncertainty of the law relating to B-party interception also requires clarification, both for law enforcement agencies and to ensure the proper protection of privacy. For the Police and the Department, the legislation represents a codification, and clarification of a situation which arguably exists at present.

4.26 The Committee notes that in many cases, those who expressed reservations about B-party warrants acknowledged that in very rare circumstances there may be some justification for them. Mr Timothy Pilgrim, Deputy Privacy Commissioner summarised the resulting dilemma:

> … we also recognise that the community expects that law enforcement agencies will have access to appropriate tools to allow them to efficiently undertake one of their key roles in the community – that of investigating criminal activities. The challenge facing the community is where to strike the right balance between these important community priorities. Is the response, for example, proportional to the risk that has been identified?[23]

4.27 Similarly, the Committee accepts the need for B-party warrants. However, the invasion of privacy of innocent parties who become the subject of surveillance merely by reason of association is very significant. The key question is therefore the extent to which the Bill provides a framework of controls over the proposed warrants to balance privacy protection with effective law enforcement.

4.28 Evidence from witnesses and submissions perceived various shortcomings and ambiguities in the B-party warrant provisions. In particular, concerns focused on:

- the differences in the thresholds for issuing B-party interception warrants and others under the legislation;
- controls on the dissemination of information beyond the B-party, and the possible derivative use of information obtained under the warrant;
- the implications for the protection of privileged communications;
- reporting and accountability requirements; and

22 *Committee Hansard*, 15 March 2006, p. 56.

23 *Committee Hansard*, 15 March 2006, p. 22.

- the need for a review of the legislation.

4.29 These issues are considered below.

Issuing B-party interception warrants

4.30 The Bill proposes two separate regimes for issuing B-party warrants: one for ASIO on application by the Director-General of Security, and another for law enforcement agencies. Evidence to the inquiry argued that the parameters for the issuance of these warrants is too wide.

Applications by the Director-General of Security

4.31 Under this proposal, B-party interception warrants could be issued to ASIO by the Attorney General (proposed Subsection 9(3)). Two issues emerged in relation to this.

4.32 The first relates to the proposed issuing authority. The Law Council was of the view that these warrants should be the subject of judicial oversight rather than being issued by a member of the executive; the council considers this is the best approach where decisions erode fundamental human rights such as interference with a person's liberty such as the unlawful interference with a person's right to privacy.[24]

4.33 In response, Mr McDonald explained that the Attorney-General has been always had responsibility for issuing telecommunications warrants, to ASIO and the safeguards which apply to other warrants issued by the Attorney will also apply to B-party warrants.[25]

4.34 The Committee notes that this measure is consistent with similar warrant regimes in the legislation; however the Committee also emphasises that these warrants are not the same as the existing TI warrants, which deal directly with persons of interest; they are third party warrants, targeted at people who may have only a very tenuous link with the person of interest.

4.35 At the same time, the Law Council's desire for judicial consideration of warrant applications appears to promote a visibly more independent approach to the issue of security warrants, although the Committee notes that in issuing a TI warrant a judge is not making a judicial decision but an administrative one.

4.36 The second matter relates to the threshold criteria for issuing the warrant. Professor Williams noted in his submission that under Item 1 of Schedule 2:

> … there is no requirement that there be evidence of a nexus between B-Party communications and the activities prejudicial to national security which triggered the warrant. All that must be shown is that: (i) the B-Party

24 *Submission* 17, p. 9.

25 *Committee Hansard*, 15 March 2006, p. 50.

> is likely to communicate with a person who is likely to engage in activities prejudicial to security; and (ii) intercepting the B-Party's communications is likely to assist in obtaining intelligence related to security.[26]

4.37 Professor Williams observes that the purpose of B-party interceptions is to assist investigations of matters prejudicial to security.[27] However, he considers the Bill grants far more extensive powers than necessary to achieve this. They may be issued in the absence of any evidence that the warrant will contribute to information about the activities which give rise to the warrant. He continued:

> It is enough to show that intercepting B-Party communications to or from *anyone* may assist in obtaining *any* intelligence related to security.[28]

4.38 Further, Professor Williams notes that the application by the Director-General must only show that the interception would be 'likely to assist' in obtaining intelligence related to security; according to Professor Williams both the terms 'likely to assist' and relating to security' are wide and vague.

4.39 The resulting powers potentially allow ASIO to engage in the kind of 'fishing expeditions' of which the Blunn report warned.[29] The B-party warrants have the potential to obtain online information on a continuous basis, allowing tracking of persons via a telecommunications device, or simply the gleaning of general information about a person's associates. If this use is intended then there should be explicit reference to it in the legislation. This breadth and vagueness could create the potential for abuse of the interception power.

4.40 Professor Williams suggested that the Bill be amended to provide for a precondition in section 9 to issuing a warrant. This would require evidence that the B-party's telecommunications service is likely to be used to communicate or receive information relevant to the particular activities prejudicial to security which triggered the warrant.

4.41 The Committee considers that this provision is far too vague. The proposal involves access to material generated by innocent persons, and must be circumscribed as far as possible to protect their privacy. The Committee notes that in comparison, search warrant regimes require applicants to establish a connection between the item sought and the offence being investigated – not to matters which are 'likely to assist'. There appears no reason why the conditions applying to warrants sought by the Director-General should not also contain analogous conditions to avoid the kind of 'fishing expedition' of concern both to Blunn and the Centre for Public Law.

4.42 Accordingly the Committee recommends:

---

26 *Submission* 2, p. 2.

27 Ibid

28 Ibid

29 Blunn, p. 74.

Recommendation 18

4.43 The Committee recommends that as a precondition to issuing a warrant under subsection 9(3), there must be evidence that the B-party's telecommunications service is likely to be used to communicate or receive information relevant to the particular activities prejudicial to security which triggered the warrant.

Applications by law enforcement agencies

4.44 Submissions to the Committee generally sought more stringent requirements for demonstrating the necessity for the B-party warrant. Electronic Frontiers Australia's submission states:

> It should be required that any agency requesting such a warrant establish to the satisfaction of the issuing authority evidence to support their belief that the information likely to be obtained from the interception is material to the investigation and that such information cannot be obtained by any means other than by interception of a B-Party telecommunications service.[30]

4.45 EFA also suggested that agencies should have to provide evidence about the type of service – business, private, high or low volume – so as to give the issuing authority relevant information to be considered when assessing the extent of the invasion of privacy of innocent party communications that is proposed. This includes not only the innocent B-party, but other innocent persons with whom the B party communicates.

4.46 Similar to EFA's first proposal, Professor Williams observed:

> Under items 8 and 9 of Schedule 2 (amending s 46), the issuing officer must be satisfied that the warrant will assist in obtaining evidence relating to the offence which is being investigated before a warrant may be issued.
>
> … These items do not, however, require that it be established that the evidence will be obtained from communications between the B-Party and the person suspected of being involved in the offence. It would be sufficient, for instance, if: (i) the B-Party sometimes communicated with the suspect; and (ii) intercepting communications between the B-Party and any third party would, in some way, assist in investigating the suspect. This is a particularly low burden.[31]

4.47 Professor Williams suggested that the preconditions for issuing a warrant under section 46 should include evidence that the 'suspect will, in some way, be causally related to communications involving the B-party which will assist in investigating the suspect.'

---

30 *Submission 3*, pp 28-29.

31 *Submission 2*, p. 3.

4.48 The Blunn report suggested that appropriate control requirements might provide that:

> … any agency requesting such a [B-party] warrant must establish to the satisfaction of the issuing authority evidence to support their belief that the information likely to be obtained from the intercept is material to the investigation. The agency should also establish that it cannot be obtained other than by telecommunications interception or the use of a listening device. It is then for the issuing authority to consider that evidence along with any other relevant matters such as the invasion of privacy involved and the gravity of the alleged offence in deciding whether to issue a warrant.[32]

4.49 When this matter was raised with the officers of the Attorney-General's Department, the Committee was advised that 'a lot of the safeguards that apply to TI more generally apply to B-party'.[33] However it emerged in discussions that the suggestion of Mr Blunn had not been taken up in drafting the bill, and that the only additional requirement applying to B-party warrants other than the general conditions was a requirement that:

> … the agency must demonstrate that it has exhausted all other practical methods of identifying the telecommunications service to be used or likely to be used by the suspect or that it is not possible to actually intercept the service being used by the suspect. That is to ensure that it is a measure of last resort and that it is done in those circumstances which are operationally required.[34]

4.50 The Committee notes that notwithstanding both the Attorney General's and the department's use of the expression 'last resort', the term does not appear in the bill, although the phrase in Schedule 2 of the bill refers to having 'exhausted all other practicable methods'.[35] Whether or not the conditions truly represent a last resort was a matter of some contention. The Law Council suggested that:

> … for the measure to be applied as a last resort, the agency should have exhausted all other means of surveillance and tracking of the suspect and not merely exhausted all other practicable methods pertaining to telecommunications services used or likely to be used by the suspect.[36]

4.51 The Council for Civil Liberties was also of the view that the process as described did not amount to a 'last resort', nor is it clear what the exhausted 'practical means' may be. Mr Murphy pointed out that this could well refer to economic efficiency or convenience.[37]

---

32 Blunn, p. 77.

33 *Committee Hansard*, 15 March 2006, p. 43.

34 Mr Gifford, *Committee Hansard*, 15 March 2006, p. 44.

35 *Committee Hansard*, 15 March 2006 p. 47.

36 *Submission* 17, p. 9.

37 *Committee Hansard*, 15 March 2006, p. 59.

Consenting to telecommunications intercepts

4.52 It was confirmed by the AFP at the hearing that the current TI arrangements do not provide for a situation where a person could consent to an intercept being placed on their service.[38] Neither is it contemplated under the current Bill.

4.53 This is not a matter that the Committee has had time to consider in adequate detail to form any conclusions. However, given the seriousness privacy implications of the B-party warrants, it is an area that deserves further consideration.

Committee view

4.54 The Committee notes that the B-party warrant is a particularly invasive tool for the detection of criminal activity. As previously acknowledged such tools may be necessary in some circumstances, but the basis for authorising them must take account of their unique nature. A B-party warrant applied to a non-suspect is simply not the same as the current regime of telephone intercept warrants applied to those suspected of serious criminal offences. The *Telecommunications (Interception) Act 1979* prescribes very closely the circumstances in which telecommunications can be intercepted, surrounding them with strict controls regarding privacy and accountability. It appears to the Committee that this aspect has been obscured where the issue of the B-party warrants is concerned.

4.55 The Committee considers that in addition to the requirements imposed under section 46(1)(a), (b), and (c) of the Act, the additional preconditions suggested by Professor Williams and Mr Blunn be included. The Committee is of the view that this will address the reservations expressed by the Law Council and EFA.

Recommendation 19

4.56 The Committee recommends that the Bill be amended to require that an applicant for a B-party warrant demonstrate:

- **evidence to support their belief that the information likely to be obtained from the intercept is material to the investigation; and,**
- **establish that it cannot be obtained other than by telecommunications interception or the use of a listening device.**

Recommendation 20

4.57 The Committee also recommends that the proposed section 46(3) (which contains the requirement that the issuing authority must not issue a B-party warrant unless he or she is satisfied that the agency has exhausted all other practicable methods of identifying the telecommunications services used) be amended to exclude the word 'practicable', to ensure that before a person is

38 *Committee Hansard*, 15 March 2006, p. 47.

subject to a B-party warrant no other way of approaching the problem is available.

Rolling warrants

4.58 The Committee heard from the Law Council that the 1979 Act included provisions for rolling over, or extending, interception warrants. The Law Council was concerned at the possibility that the same might apply to the B-party intercepts:

> When you think about rolling over interception warrants in relation to innocent people, the mind boggles. We believe that there should not be any rollover unless a judicial officer can be shown that some very useful or crucial information from an earlier warrant was gained.[39]

4.59 Rolling warrants allow a warrant to be renewed before the original warrant has expired. Their use is circumscribed, and the Attorney General's Department explained in evidence that provisions which apply to the stored communications warrants under this bill do not permit the use of rolling warrants for stored communications.[40] However, there does not appear to be a similar prohibition on rolling B-Party warrants.

4.60 The Committee considers, given the nature of these warrants, that the Bill should be amended to state specifically that the B-party interception warrants cannot be renewed under any circumstances. Instead, if further interception is required after a warrant expires, it should be the subject of a fresh application.

Recommendation 21

4.61 The Committee recommends that the Bill be amended to state that B-party interception warrants cannot be renewed. If further interception is required after a warrant expires, it must be the subject of a fresh application.

Dissemination and subsequent use: legal and other professional privilege

Use and derivative use

4.62 A principal problem with the B-party warrant is the potential for collecting a great deal of information which may be incidental to, or not even associated with the investigation for which the warrant was issued. As Senator Ludwig noted, 'it is not only the B-party but also the C, D E and F parties who may at some point end up talking to B and, therefore, being captured'.[41] The result is that potentially not just one, but a great many non-suspects to be caught in the B-party warrant process.

---

39 *Committee Hansard*, 15 March 2006, p. 29

40 *Committee Hansard*, 15 March 2006, p.40

41 *Committee Hansard*, 15 March 2006, p. 29.

4.63 The subsequent use of such material obtained does not appear to be controlled. This was confirmed to the Committee in response to a question from Senator Ludwig in which Mr McDonald of the Attorney General's Department affirmed that use and derivative use would be permitted of the material obtained under a B-party warrant relating to a non-suspect.[42]

4.64 Mr Gifford explained that this is consistent with the way that a service or named person warrant currently operates:

> … you may be the target of the interception and conversing with Senator Payne, and Senator Payne is not a target of the investigation at all. But Senator Payne may talk about another offence that was not the subject of the original investigation, to the extent that the original warrant was justified to and authorised by the issuing authority. Then any criminal intelligence which is subject to a three-year penalty threshold can be used.[43]

4.65 Mr Gifford explained the implications of limiting the use of this material. He continued:

> The reverse situation would require destruction of very valuable criminal information. The extreme example would be that you would happen upon some very valuable information in terms of a terrorism investigation. That is an extreme example, but the use of that information is useful for our operational agencies and has been justified in terms of the initial warrant being authorised by the issuing authority.[44]

4.66 It could be argued that the terms of the warrant itself would dictate the limits of the use of information obtained, but given the potential breadth of the information able to be sought under items 8 and 9 of Schedule 2 (amending section 46), and in the light of the remarks made by Professor Williams discussed above, it is likely that a great deal of what the Hon Duncan Kerr MP calls 'collateral information' will be collected, and therefore available for use.[45]

4.67 The Law Council of Australia, while maintaining its concerns regarding the B-party warrants, said that proper controls are necessary to regulate use and derivative use.[46] Professor Williams also supported stricter controls:

> My view is that it is better to be safe than sorry in an area like this, and it is very difficult through destruction only to be absolutely clear that the immunities you would expect to apply in such circumstances actually do apply. In the same way, it is common to see immunities, whether it be in the ASIO legislation or other bits of legislation, recognising that information

---

42 *Committee Hansard*, 15 March 2006, p. 51.

43 *Committee Hansard*, 15 March 2006, p. 51.

44 Ibid.

45 *Submission 1*, p. 4

46 *Committee Hansard*, 15 March 2006, p. 6.

> can be collected inadvertently, otherwise it should not have been collected. I would prefer to see a clear, direct statement indicating that, if it does not fit within the information that could have been collected for a certain purpose, immunities apply. I think it is inappropriate for enforcement agencies, simply through their luck or overboard legislation, to get access to information and then use it. [47]

4.68 Further, the fact that these warrants collect material about third parties who are not suspects must demand particular conditions about the use of any information obtained.

Professional privilege – legal and otherwise

4.69 A particular problem in this potentially open-ended process, concerns that of professional privilege. While the discussion centred upon legal professional privilege, the confidential nature of telephone contact with doctors, family members and other professionals was raised. Ms Irene Grahame[48] indicated that EFA already believes that there is a problem with the existing interception warrants and that the B-party warrants represent an even greater problem because of the issue of legal professional privilege. Ms Grahame continued:

> It is ridiculous to think that people would no longer be able to be confident in seeking legal advice because their lawyer's phone was being intercepted. … Any extension of it, in our view, would have to make very clear that B-parties could not cover lawyers, because there is too much potential for people who are not a suspect and the lawyer who is not the suspect having their calls intercepted. [49]

4.70 Ms Grahame also considered the possibility of such an exception also applying to other people who have a large number of calls, including politicians and accountants.[50]

4.71 Professor Williams took the view that:

> … unless there are particular or special circumstances, privileged information, such as lawyer-client information, ought not be collected through this type of regime. There are good arguments whereby, if lawyers themselves were involved in activity that may be criminal or otherwise, that may well negate the privilege. I could accept that there may be reasons why it should be collected on that basis. Otherwise, the very nature of lawyer-client privilege is that, where the government itself tends to be the party on the other side of the litigation table, it is highly inappropriate that the government gets access to that very information. It casts into doubt the

47 *Committee Hansard*, 15 March 2006, p. 30.

48 *Committee Hansard*, 15 March 2006, p.14

49 *Committee Hansard*, 15 March 2006, pp 9-10.

50 *Committee Hansard*, 15 March 2006, p.10

> justice system in terms of how that information is used. It can lower public confidence and, except in those limited circumstances, I would prefer to see a clear exception for that type of information.[51]

4.72 In pursuing this issue with the Attorney-General's Department, the Chair of the Committee asked about the interception of conversations between individuals and legal representatives, medical practitioners or clergy.[52]

4.73 In response, Mr McDonald of the Attorney General's Department indicated that in the case of *Carmody v MacKellar Ors*[53] the full Federal Court held that legal professional privilege was excluded by implication under the current warrant provisions of the TI Act. By extension, the privilege is excluded under the B-party warrant regime, even though these warrants are specifically directed against innocent parties.

Committee view

4.74 The Committee remains most concerned at the potential breadth of information relating to individuals suspected of no criminal offence which could be captured under the B-party warrants. The Committee does not consider that the provisions which operate for other warrants under the Act are adequate for this unique situation.

4.75 The Committee notes the comments made by Professor Williams in discussion of the use implications and those for legal professional privilege:

> I would prefer to see a clear, direct statement indicating that, if it does not fit within the information that could have been collected for a certain purpose, immunities apply. I think it is inappropriate for enforcement agencies, simply through their luck or overboard legislation, to get access to information and then use it.[54]

4.76 The Council for Civil Liberties agreed:

> [I]f you are going to provide this power then you need to provide an immunity so that anything that is not directly related to the investigation for which the warrant has been obtained needs to be expressly excluded from being used in evidence against anybody else.[55]

4.77 The Law Council's recommendations supported the need for limitations:

> g. The measures should contain express exemption categories. Exempt communications should include the confidential communications with lawyers, doctors and the clergy;

---

51 *Committee Hansard*, 15 March 2006, p. 29

52 *Committee Hansard*, 15 March 2006, p. 45.

53 [1997] 839 FCA

54 *Committee Hansard*, 15 March 2006, p. 30.

55 *Committee Hansard*, 15 March 2006, p. 58.

h. The proposed measures should expressly provide that Schedule 2 does not abrogate Legal Professional Privilege;[56]

4.78 The Committee is aware that these amendments are designed to meet some of the demands which are a function of modern technology, and acknowledges that law enforcement agencies are constantly meeting situations which demand sophisticated technical responses. Nevertheless, it is important to keep in mind the purpose behind the principle of legal professional privilege: that the law and the system of justice that administers it, is complex and that those affected by it are in need of professional assistance. In seeking such assistance, the client must be able to reveal all the relevant facts without inhibition, in order to get effective advice.[57]

4.79 So long as the communications are legitimately for the purpose of gaining professional legal advice, they should be protected in the normal way. In addition, there is little benefit in creating rules against the admissibility of such evidence if, in fact, law enforcement agencies have been privy to the confidential information already.

Recommendation 22

4.80 The Committee recommends that Schedule 2 be amended to provide that certain material obtained under a B-party warrant will be exempted from use under the legislation. This material should include bona fide communications between solicitor and client; clergy and devotee; doctor and patient and communications by the innocent person with any person other than the person of interest to the law enforcement agency.

Recommendation 23

4.81 The Committee further recommends that the Bill be amended to introduce defined limits on the use and derivative use of material collected by B-party warrant.

Reporting and accountability requirements

4.82 A matter of vital importance to the workability of the proposals is the strength of the reporting and accountability regime, particularly in view of the covert nature of the warrant system proposed. Warrants granted under Part III and Part VI would have differing reporting and accountability requirements.

B-party warrants issued on application of the Director-General of Security

4.83 The Inspector-General of Intelligence and Security has a statutory obligation under the *Inspector-General of Intelligence and Security Act 1986:*

56 Submission 17, pp 3-4.

57 Gillies, P., *Law of Evidence in Australia*, p. 433.

a) to assist Ministers in the oversight and review of:

(i) the compliance with the law by, and the propriety of particular activities of, Australian intelligence or security agencies;

(ii) the effectiveness and appropriateness of the procedures of those agencies relating to the legality or propriety of their activities; and

(iii) certain other aspects of the activities and procedures of certain of those agencies;

(b) to assist Ministers in ensuring that the activities of those agencies are consistent with human rights; and

(c) to allow for review of certain directions given to ASIO by the Attorney-General. [58]

4.84 There is no existing requirement for telephone intercept warrants issued by the Attorney and associated documents to be destroyed, but monitoring and inspection regimes do apply.

4.85 In his submission to this inquiry, Mr Ian Carnell, the Inspector-General of Intelligence and Security indicated that his office conducts monthly inspections of all requests by ASIO for telecommunication interception (including named person) warrants under the TI Act.

> In addition to this, the office of the IGIS also inspects all requests for questioning and detention, entry and search, listening device, computer access and computer access warrants sought under the *Australia Security Intelligence Organisation Act 1979* (ASIO Act).[59]

4.86 In scrutinising ASIO's requests for warrants, the office of the IGIS checks *inter alia*, that the intelligence or security case is soundly based, and all appropriate internal and external approvals have been obtained.

4.87 The scrutiny also extends to the timely provision of factual reports to the Attorney-General of the outcome of executed warrants and checking that the activity concerned occurred only during the approved period.

4.88 Mr Carnell noted that both the B-Party interception and equipment-based interception will be subjected to this inspection regime; he also observes that:

> … the nature of B-Party interception warrants inherently involves a potential for greater privacy intrusion for persons who may not be involved in activities of legitimate concern under the ASIO Act. As a result, particular attention will be given to the additional legislative tests for this type of warrant. As a result, particular attention will be given to the

58 Section 4

59 *Submission* 9, p. 2.

> additional legislative tests for this type of warrant, as well as checking that the duration of 90 days is adhered to.[60]

B-party warrants issued on the application of a law enforcement agency

4.89 For the B-party warrants issued by Judges and members of the AAT, the reporting, destruction and supervising arrangements are the same as those which currently apply to telephone intercepts. Briefly, sections 79, 80 and 81 prescribe the circumstances under which records are to be destroyed, and the records that must be kept of notifications and certification of warrants, outcomes and use of information obtained under the warrant.

4.90 In evidence, Mr Gifford of the Attorney General's Department explained:

> The use and destruction provisions that are currently in the existing *Telecommunications (Interception) Act* will apply to B-party interception. It was a conscious decision by the Attorney-General that they would be maintained… The *Telecommunications (Interception) Act* currently requires the destruction of material once the general and special registers of warrants have been inspected by the Attorney-General. Those registers are compiled three-monthly by the AFP. After they are reviewed and signed off by the Attorney-General then a notice is provided to all agencies, at which point they may destroy all material that is contained in the general and special registers.[61]

4.91 The Explanatory Memorandum to the Bill explained:

> Lawfully obtained information obtained as a result of B-Party interception will be subject to the existing destruction provisions of the Act, namely, destruction where the permitted purpose for use cease to exist.[62]

Criticisms of the accountability regime

4.92 Several submissions pointed to weaknesses in this regime. Electronic Frontiers Australia said in their submission that the current arrangements for destruction have been ineffective since 2000:

> The existing destruction provisions apply only to 'restricted records' which has not included copies of intercepted communications since amendments made in 2000. Hence copies of irrelevant intercepted information, e.g. communications between the innocent B-Party and other innocent persons, will be permitted to be retained forever due to the inadequate destruction provisions of the existing Act.[63]

---

60 Submission 9, pp 2-3.

61 *Committee Hansard*, 15 March 2006, pp 50-51.

62 Explanatory Memorandum to the Telecommunications (Interception) Amendment Bill 2006, p. 32.

63 *Submission* 3, p. 28.

4.93 The Privacy Commissioner also expressed disquiet at the provisions for destruction, recommending 'enforceable, audited requirements that any intercepted material outside the scope of the purpose stated in the warrant be immediately destroyed.'[64]

4.94 The Law Council[65] and EFA[66] made substantively similar recommendations which suggested that the government should be required to report annually on specific details of B-party warrants including:

- the number and justification of B-party intercept warrants (which should be separately recorded by the Agency Co-ordinator and reported to the Attorney General);
- the number of warrants issued by the Attorney General, judicial officers and nominated AAT Member pursuant to schedule 2, and including the grounds upon which they were issued;

4.95 EFA also recommends that the reporting requirements should include the suggestion made in the Blunn report that destruction of non-material content in whatever form should be strictly supervised. [67]

4.96 The Committee endorses the proposals to improve security and accountability in relation to B-party warrants, and reiterates its view that the proposals cannot be treated as being analogous to the current TI warrant arrangements.

Recommendation 24

4.97 The Committee recommends that:

- **there should be strict supervision arrangements introduced to ensure the destruction of non-material content in any form;**
- **the number and justification of B-party intercept warrants should be separately recorded by the Agency Co-ordinator and reported to the Attorney General; and**
- **the use of such warrants should be separately reported to the Parliament.**

Role of the Ombudsman

4.98 A further consideration that relates specifically to law enforcement agencies is the role of the Commonwealth Ombudsman. The overall inspection of interception warrant records is the responsibility of the Ombudsman under Section 82 of the *Telecommunications (Interception) Act 1979*. Under the Act, the Ombudsman's role is

64 *Submission* 6, p. 2.

65 Submission 17, p. 4

66 *Committee Hansard*, 15 March 2006, p. 9

67 *Submission* 3, p. 28

to inspect and report on the records of telecommunications interception activity by the Australian Federal Police and the Australian Crime Commission.[68]

4.99 The Ombudsman explained:

> Section 83 of the Act requires the Ombudsman to inspect each of these agency's records at least twice in each financial year to ascertain the extent to which they have complied with the provisions of sections 79, 80 and 81 of the Act dealing with the destruction and maintenance of records. Under section 85, the Ombudsman may also report on any other breaches of the Act detected in the course of an inspection. Under section 84, the Ombudsman is required to report to the Minister within three months after the end of each financial year about the results of the inspections conducted under section 83 in relation to each agency during that financial year. As a consequence of amendments to the Act which came into effect in July 2005, I am now required to include in my annual report to the Minister particulars of any deficiencies identified in those inspections that may impact on the integrity of the telecommunications interception regime and particulars of any remedial action taken or proposed to address those deficiencies.[69]

4.100 While there are no specific requirements for the Ombudsman to investigate particular aspects of the B-party warrants subject to certain provisions of the Act, the Ombudsman can undertake own motion investigations under the *Ombudsman Act 1976* into other matters relating to the conduct of telecommunications interceptions by law enforcement agencies.

4.101 It is theoretically open to any person adversely affected by the B-party warrant provisions to notify the Ombudsman, in the case of an agency, or the IGIS in the case of an ASIO warrant. However, the nature of the provisions and the covert nature of the surveillance makes it most unlikely if not impossible for such a notification to occur. As the Committee Chair noted in the public hearing:

> I am not entirely persuaded that one can complain to the Ombudsman or the IGIS about a telephone intercept that one does not know about. [70]

4.102 As discussed in the previous chapter, in view of the additional warrants which the Ombudsman is required to inspect and report on, the Committee is concerned to ensure that sufficient resources are at the Ombudsman's disposal. The Ombudsman remarked:

> The Ombudsman's inspection and reporting role is an important safeguard in ensuring that these powers are not misused and in maintaining public confidence in the integrity of the new warrant regime. It would be contrary

68 *Submission* 10, p. 1.

69 Ibid.

70 *Committee Hansard*, 15 March 2006, p. 50.

> to the intent of the legislation if this office were forced to curtail these activities for want of resources to fulfil this role.[71]

4.103 The Ombudsman continued:

> Whether my office is able to inspect most, if not all, agencies, in the spirit of the proposed amendments, or whether we will be able to inspect only a few, will depend on whether additional resources are available. Not only will staff need to be available to carry out inspections but preparatory work on methodologies and the internal procedures of each agency to be inspected will need to be done. If the resources are available to meet both my mandatory inspection obligations and my function under proposed section 152, my aim would be to have a program of inspections covering all agencies which have accessed stored communications in the relevant year. [72]

4.104 Accordingly, the Committee reiterates its previous recommendation relating to the adequacy of funding to the Commonwealth Ombudsman.

Review of the legislation

4.105 A number of submittors and witnesses suggested that there should be a review of the legislation after a period of time, or the inclusion of a sunset clause.

4.106 The Law Council of Australia said that 'similar to other legislation which erodes fundamental rights of the Australian people', Schedule 2 should be subject to independent review, for instance, two or three years after its commencement; and 'a sunset clause should be incorporated in the Act'.[73]

4.107 In evidence, Mr Cameron Murphy of the Council for Civil Liberties agreed that a sunset clause coupled with a review would ensure that the conditions which support the introduction of these provisions are continuing.[74]

4.108 Mr Blunn's report considered further reviews inevitable:

> Indeed given the rate of changes within the industry and within society more generally I believe that there is a strong case for regular reviews, say at three yearly intervals. The complexity and significance of the issues makes it problematic for unversed persons to do justice to them within a reasonable time frame. I am not a fan of committees but there may be

71 *Submission* 10, p. 4.

72 Submission 10, p. 2

73 *Submission* 17, p. 3.

74 *Committee Hansard*, 15 March 2006, pp 59-60

> advantage in there being a standing representative committee structure which could do or at least provide support for future reviews.[75]

4.109 Dr Clapin, from the Office of the Privacy Commissioner said in evidence that such a review should not be limited to these provisions, but to the entire Act and that provision should be made in these amendments.[76]

Committee view

4.110 The Committee considers a sunset clause to be appropriate for the B-party interception warrant provisions; it would serve as a catalyst for a review of the whole telecommunications interception structure, and in the light of advancing technology would offer an opportunity to assess the adequacy or otherwise of this regime.

Recommendation 25

4.111 The Committee recommends that the Bill should include a provision for the provisions to expire in five years, with a review at that time or earlier.

4.112 The Review should encompass the broader issues surrounding the suitability and effectiveness of AAT members in the warrant issuing regime, together with consideration of ways in which the Act may be amended to take account of emerging technologies such as peer-to-peer technology.

Equipment based interception

4.113 Schedule 3 to the bill deals with the provisions concerning equipment-based interception.

4.114 Under current law, it is possible to apply for a TI warrant for a named person, which allows interception of phone services attached only to that particular person rather than to a specific device. This has been a source of difficulty for law enforcement agencies, when targets of interception use a multitude of different SIM cards or phone numbers that may not be registered in their name.

4.115 The Explanatory Memorandum states:

> The purpose of this Schedule is to amend the named person telecommunications interception warrant provisions to enable interception agencies to intercept communications to and from communications equipment such as mobile handsets and computer terminals. These amendments are designed to assist interception agencies to counter measures undertaken by persons of interest to evade telecommunications interception such as adopting multiple telecommunications services.[77]

---

75 Blunn, p. 2.

76 *Committee Hansard*, 15 March 2006 p. 22.

77 Explanatory Memorandum, p. 34.

4.116 The proposed warrants will only be issued where the agency can show that there are no other practicable methods of identifying the device. The issuing authority must be satisfied that the applicant agency 'has no practicable methods of identifying the telecommunications services used or likely to be used by the person of interest, or that interception of those services would not be possible.'[78]

4.117 The provisions are designed to gain access to an individual piece of equipment-such as a computer or a mobile phone, via a unique identification number. In evidence, Ms Hume from the Attorney General's Department explained:

> Proposed section 6Q in schedule 3 … talks about the identification of a telecommunications service. In both subsections (a) and (b) it refers to a unique telecommunications number. In item 3 the list of those numbers shows that potentially it could be a telephone number. It could be an IMEI[79] … It could be a MAC address of a computer. But that provision, 6Q, specifies that it has to be unique; it is a unique telecommunications number.[80]

4.118 However Electronic Frontiers Australia considered that such unique identifiers are unreliable. The submission recommended that the Schedule be deleted from the bill:

> This proposal appears to have an inappropriately and unjustifiably high potential to result in interception of communications of persons who are not suspects (i.e. are not named in the warrant) because, among other things, the types of device numbers proposed to be used do not necessarily uniquely identify a particular device.[81]

4.119 EFA notes that while the Blunn report briefly discussed equipment-based interception proposals, he made no recommendation that the warrants be implemented. Rather, his recommendation proposed:

> that priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.[82]

4.120 In evidence, it became clear that there was a sound basis for EFA's concerns. Mr Gifford of the Attorney General's Department acknowledged that there is potential for duplication of numbers thought to be unique:

> We do understand that risk, and we are aware that there are duplicate IMEIs in a telecommunications network. On that basis, we have said, 'When you're seeking interception on the basis of a handset, it must be defined by reference to a unique telecommunications number, which, for the purposes

78 Ibid.

79 International Mobile Equipment Identifier

80 *Committee Hansard,* 15 March 2006, p. 55

81 EFA, *Submission 3*, p. 28

82 Blunn, p. 46.

> of the definition, will include an IMEI. … You must satisfy the issuing authority that the IMEI you are seeking interception of is a unique IMEI number.[83]

4.121 Deputy Commissioner Lawler explained that:

> … we have seen a practice whereby these numbers have been copied fraudulently within service providers to commit fraud, but also to enable another way of not being able to identify who has the particular handset in question. I understand from the briefings I have received that there is the capacity to remove such duplicate numbers from the system, as there is also the capacity to remove stolen handsets from the system. As has been indicated, we would do the checks that are required for the potential for those numbers to be duplicated on the system, but they are only duplicated through, as I am briefed, a fraudulent activity and the numbers being cloned or copied.[84]

4.122 In further discussion, the AFP indicated that they would be required to undertake inquiries regarding the uniqueness of the proposed identifier, and to provide details in any application for a warrant the steps which had been undertaken to achieve this.[85] The Committee notes that it was not clear from the evidence the extent to which that process would guarantee that the device being targeted under the warrant was able to be certified as uniquely identifiable.

4.123 The Privacy Commissioner also had reservations about Schedule 3, observing that it 'broadens the ways in which law enforcement agencies may seek to intercept communications under the Interception Act.'[86] While acknowledging that the proposals offer a practical solution in instances where multiple SIM cards are used on the one handset:

> … the provisions in Schedule 3 appear to move beyond just permitting interception of particular mobile phone handsets, for example in permitting telecommunications equipment to be identified on the basis of an email address or a 'user account identifier'.[87]

4.124 The Privacy Commissioner concluded:

> The Office has not been able to fully determine the limits to the scope of the operation of Schedule 3, and so recommends that careful consideration be given to ensuring that the provisions of Schedule 3 do not give rise to an unintended reduction of the privacy protections in the Interception Act.[88]

---

83 Mr Gifford, *Committee Hansard*, 15 March 2006, p. 54

84 Federal Agent Lawler, *Committee Hansard*, 15 March 2006, p. 54

85 *Committee Hansard*, 15 March 2006, p. 55

86 *Submission* 6, p. 3.

87 Ibid

88 Ibid

Committee view

4.125 The Committee considers that any arrangement designed to target a specific piece of equipment should be able to identify it with a high degree of certainty. It is the Committee's view that while there is a clear operational requirement for law enforcement agencies to be able to target specified devices, doubts remain over their capacity to identify these devices with a high degree of certainty. As Mr Blunn recommended, priority should be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access. However, the Committee also recognises that such developments may take some years to achieve and does not consider it practicable to delay the passage of the provisions until that time.

Recommendation 26

4.126 The Committee recommends that the recommendation contained at paragraph 3.2.5 of the Blunn report be adopted, and priority given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.