The Parliament of the Commonwealth of Australia

Senate Legal and Constitutional Legislation Committee

Consideration of legislation referred to the Committee

Inquiry into the Provisions of the Telecommunications (Interception) Legislation Amendment Bill 1999

MAY 2000

ISSN 1326-9364

This document was produced from camera-ready copy prepared by the Senate Legal and Constitutional Legislation Committee, and printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

Members of the Legislation Committee

Members

Senator M Payne, New South Wales, *Chair*

Senator J McKiernan, Western Australia, *Deputy Chair*

(Senator J Ludwig in substitution for Senator McKiernan for the period 17 April to 8 May 2000)

Senator H Coonan, New South Wales

Senator B Cooney, Victoria

Senator B Mason, Queensland

Senator B Greig, Western Australia

Participating Members

Senator the Hon. E Abetz, Tasmania

Senator the Hon. N Bolkus, South Australia

Senator the Hon. D Brownhill, New South Wales

Senator G Chapman, South Australia

Senator A Eggleston, Western Australia

Senator A Ferguson, South Australia

Senator the Hon. B Gibson, Tasmania

Senator S Knowles, Western Australia

Senator J McGauran, Victoria

Senator N Stott Despoja, South Australia

Senator J Tierney, New South Wales

Senator A Bartlett, Queensland

Senator B Brown, Tasmania

Senator P Calvert, Tasmania

Senator W Crane, Western Australia

Senator the Hon. J Faulkner, New South Wales

Senator J Ferris, South Australia

Senator B Harradine, Tasmania

Senator R Lightfoot, Western Australia

Senator the Hon. W Parer, Queensland

Senator T Tchen, Victoria

Senator J Watson, Tasmania

Secretariat

Dr Pauline Moore (Secretary to the Committee)

Mr Noel Gregory (Principal Research Officer)

Ms Saxon Patience (Executive Officer)

PARLIAMENT HOUSE

CANBERRA ACT 2600

Tel: (02) 6277 3560

Fax: (02) 6277 5794

TABLE OF CONTENTS

FOREWORD

Despite advertising the inquiry and writing to various bodies inviting submissions, the Committee received very few submissions from non-user organisations whose major interest is assumed to be in issues of individual privacy. This lack of information may mean that the Bill is generally regarded as not unduly threatening that privacy. Be that as it may, the limited information presented on such matters reduces the Committee's capacity to investigate matters such as the adequacy of reporting mechanisms. The first recommendation arises from this:

Recommendation 1

The Committee **recommends** that the Bill provide for a review of its operations within three years of coming into effect. This review is to have regard to the matters considered in the current reference to this Committee.

As appears at paragraph 2.25, it is not made clear in the Bill that intercepted information given in evidence in exempt proceedings may only be used in subsequent proceedings subject to the general rules of admissibility.

Recommendation 2

The Committee **recommends** that a note be inserted in the Bill to make it quite clear that proposed section 75A is subject to the general rules of admissibility.

The Committee was not satisfied that the criticisms made of the Bill were justified. It is satisfied that there is a need for named person warrants and that the Bill seeks to balance the needs of user-agencies and the right to privacy of individuals.

Recommendation 3

The Committee **recommends** that the Bill proceed without amendment.

Senator Jim McKiernan

Deputy Chair

Legislation Committee

May 2000

CHAPTER ONE

BACKGROUND

The Inquiry

1.1 The *Telecommunications (Interception) Legislation Amendment Bill 1999* (the Bill) was introduced into the House of Representatives on 16 February 2000. The Senate referred the provisions of the Bill to the Legal and Constitutional Affairs Legislation Committee on 8 March February 2000, for inquiry and report by 11 May 2000.

1.2 The Committee has been tasked with an inquiry that, among other issues, considers the following:

- the need for a new warrant;
- the adequacy of safeguards; and
- the adequacy of reporting mechanisms.

The Bill

1.3 The Explanatory Memorandum states that the Bill has its origins partly in the Telecommunications Interception Policy Review (the Review) and partly in practical operational difficulties arising from rapid change in the telecommunications industry.[1] The Review[2] was tabled in the Parliament on 25 August 1999.

1.4 The Explanatory Memorandum states that rapid changes in technology, coupled with competition in the telecommunications market, allow customers to choose from a variety of services and means of communication.[3] Because the *Telecommunication (Interception) Act 1979* (the Principal Act) is currently structured on the premise that a warrant relates to one, identified telecommunications service, it requires an agency wishing to intercept all the telecommunications services used by a particular suspect to obtain a separate warrant for each service. The Bill will up-date the Principal Act to enable connections, disconnection and reconnection in rapid succession of interceptions of multiple services (used by a particular suspect in connection with the same matter) without the need to obtain a fresh warrant each time.[4]

1.5 The Bill provides for 3 types of warrant:

---

1 Explanatory Memorandum, p. 1.

2 This review was conducted by Mr Peter Ford, First Assistant Secretary, Information and Security Law Division, Commonwealth Attorney-General's Department.

3 Explanatory Memorandum, p. 2.

4 For example, a person may subscribe to multiple services by acquiring several pre-paid mobile telephone services which may be used in the one telephone handset, and swapped around and discarded at will.

- The existing single service warrant, usable by ASIO in relation to security or by law enforcement agencies in relation to crime;
- The named person warrant authorising the interception of any telecommunication service that the person named on the warrant uses or is likely to use. It also will be usable by ASIO in relation to security and by law enforcement agencies in relation to crime; and
- The foreign intelligence warrant, not limited to specific services or specific persons, usable only by ASIO in relation to specified foreign intelligence.[5]

1.6 The Explanatory Memorandum says that the Bill will not diminish the safeguards in the Principal Act and that the existing procedures and criteria for the issue of a warrant and the record-keeping and reporting requirements apply in full. In addition, the authority issuing a named person warrant must be satisfied that a telecommunications service warrant is unavailable, or would be ineffective. The agency must report on such matters as the services intercepted and the reasons why it was ineffective to use a telecommunications service warrant.[6]

1.7 The Explanatory Memorandum also states that the Bill will:

- remove the requirement that warrants authorising entry onto premises as well as interception be executed by the Australian Federal Police;
- allow intercepted material lawfully disclosed in an exempt proceeding to be used in subsequent proceedings; and
- enable intercepted information to be used in proceedings for the review of a decision to grant bail.[7]

Conduct of the inquiry

1.8 The Committee wrote to a range of individuals and organisations and advertised in a national newspaper on 18 and 19 March 2000. In response, the Committee received 11 submissions, including one that was confidential. A list of non-confidential submissions is at Attachment 1. The Committee held a public hearing in Sydney on Thursday, 27 April 2000. A list of the witnesses at that hearing is at Attachment 2.

1.9 The Committee notes its concern at the low level of participation in the inquiry by peak legal bodies and bodies focused on the privacy of the citizen. This may be attributed to factors such as the specialised nature of the legislation, and the short time frame allowed by the Senate for the inquiry. This latter point was noted by the Queensland Law Society Inc, the Law Institute of Victoria and Australian Women Lawyers**,** and the Committee acknowledges that in some instances short legislation reporting dates have hampered effective inquiry. The Committee again wishes to bring this matter to the attention of the Selection of Bills Committee in the Senate, advising that Committees with several inquiries often require additional time to enable them to address matters at an appropriate level.

---

5 Explanatory Memorandum, pp. 3-4.

6 Explanatory Memorandum, pp. 3-4.

7 Explanatory Memorandum, p. 4.

1.10 The limited input from experts put the Committee at some disadvantage, including only being able to take evidence from the policy department[8] and user-bodies which intercept telecommunications.

Recommendation 1

The Committee **recommends** that the Bill provide for a review of its operations within three years of coming into effect. This review is to have regard to the matters considered in the current reference to this Committee.

Note on references

1.11 References to submissions are to individual submissions as received by the Committee, and not to a bound volume. References to the Hansard transcripts are to the proof Hansard. Page numbers may vary between the proof and the final Hansard transcript.

8 Commonwealth Attorney-General's Department.

CHAPTER TWO

ISSUES RAISED BY THE BILL

Telecommunications interception in general

2.1 Agencies were generally enthusiastic about the use of telecommunications interception.

> . . . in regard to the effectiveness of TI, from an investigative point of view we believe it is an incredible tool.[1]

2.2 Similar support was given by Commissioner Palmer of the Australian Federal Police:

> the quality of evidence in the event of a successful strike and the corroboration or circumstantial evidence it otherwise possibly gives to police are very significant. I think the high level of guilty pleas that has resulted from very serious arrests in recent times in this country is a reflection of the quality of that sort of technological evidence in surveillance terms, in listening device terms and in telephone interception terms. It is causing people who refuse to speak to police, who are never likely to take part in an interview and who have not been touched by police in 25 years of criminal activity to plead guilty in the face of one apprehension.[2]

Need for named person warrants

2.3 There was general agreement among user-agencies that, in the absence of named person warrants, criminals had left them behind in the technological race.[3] Commissioner Palmer said:

> The main thrust of the amendments is to attempt to allow law enforcement to regain and then retain the level of efficiency and effectiveness that was intended when the (Telecommunications (Interception)) Act was first enacted in 1979. Having regard to the huge changes in technology . . . the reality is that law enforcement has lost a lot of ground in terms of its capacity to intercept communication among properly identified suspects of serious crime from the days when it was a fairly simple exercise of taking off the home phone and the office phone and then having access to most of the communications'.[4]

---

1 *Transcript of evidence*, Victoria Police, p. 19.

2 *Transcript of evidence*, Australian Federal Police, p. 4.

3 *Transcript of evidence*, Australian Federal Police, pp. 1-2; *Transcript of evidence,* National Crime Authority, p.3, *Transcript of evidence,* Australian Security Intelligence Organisation, p. 6. See also *Transcript of evidence,* Attorney-General's Department, page 5.

4 *Transcript of evidence*, Australian Federal Police, p. 1.

2.4 A number of submissions specifically described the manner in which the changes in technology had left law enforcement behind in terms of its capacity to intercept communications.FN4A[5]. For example, the Attorney-General's Department stated:

> The main benefit of competition in the telecommunications industry is the increased number of service providers that individuals may choose from. Customers may now choose from a variety of services and means of communication - fixed telephones, mobile telephones, pagers and computers connected to the Internet. In the case of mobile telephones, a person can subscribe to multiple services simply by acquiring several pre-paid services which may be used in the one telephone handset, and swapped around and discarded at will.[6]

The National Crime Authority illustrated the problem in the following way:

> Investigations undertaken by the 19 law enforcement agencies participating in the Blade National Task Force (the coordinated national effort against South East Asian Organised Crime) have noted the increasing use of multiple SIM cards (usually obtained under false identities) and multiple mobile phone handsets amongst persons involved in heroin trafficking. Persons under investigation freely switch mobile phones and SIM cards using an array of phone and SIM card combinations.[7]

2.5 It was stated by one witness that it could take up to a week, perhaps longer, to obtain a warrant.[8] Another witness gave evidence that, for the Victoria Police, the turnaround time for a warrant was between 3 and 7 days. Under the current system, they could keep up with a person moving from one phone to another as long as the time frame did not fall under 3 days. However, over the last 12 to 18 months, they had noticed that targets were moving a little more quickly.[9] If the police had a named person warrant and the target changed to a new service, it would take at most 24 hours, down to half a day, to monitor a hardline service or probably half an hour to monitor a mobile service.[10]

2.6 Evidence was given that one benefit of named person warrants would be the ease of proving in a prosecution that the correct processes had been followed where more than one service was involved:

> There are a lot of master tapes, there are a lot of disks around and there is a lot of recording equipment. To put everything together is messy.
>
> The warrant against the person could alleviate a lot of these concerns because you would basically have one recording disk, one warrant and all the services. All the

---

5 *Submission No 1A*, New South Wales Police Service, p. 2; Submission No 2, Independent Commission against Corruption, p. 1.

6 *Submission No 6*, Attorney-General's Department, p.4.

7 *Submission No 5*, National Crime Authority, p. 3. The SIM card (the Subscriber Identity Module Card) is the means by which the Global System for Mobiles is accessed. It enables a system to be identified for the purposes of calling, billing, etc.

8 *Transcript of evidence*, New South Wales Police Service, p. 16.

9 *Transcript of evidence*, Victoria Police, p. 19.

10 *Transcript of evidence*, Victoria Police, p. 20.

> lines you were intercepting would be on the one modem . . . So, for evidentiary purposes, it is worth while for us to have one single system in place.[11]

2.7 However, there was some disagreement among agencies about the likely rate of use of named person warrants. It was noted that the use of equivalent warrants in the United States was claimed to be extremely rare,[12] a point substantiated by the Attorney-General's department.[13] However, the department advised that in quite a significant minority of cases, something like 10 or 20 per cent, the FBI and Justice Department did run up against the same problems that the Bill was addressing.[14] One of the reasons for this pattern in the United States was that the country had largely stayed with the analog system and had not embraced the new technology on the same scale as Australia:

> I am not saying that they are not using prepaid SIMs, but their analog network over there is still operating and far more extensive than their digital infrastructure.[15]

2.8 The need for warrants was demonstrated, according to the Victorian Police, by the fact that probably 30 to 40 per cent of their current warrants would cover targets swapping across multiple services.[16] The New South Wales Police Service gave evidence that 30 per cent of their jobs were related to prepaid swapping.[17]

The adequacy of safeguards

2.9 The Committee is satisfied as far as it can be in the circumstances with the adequacy of the safeguards in the Principal Act and Bill. However, as noted above at Paragraph 1.9, the Committee would have appreciated being informed by more submissions from non-user agencies.

Criteria for issue of named person warrants

2.10 The criteria for issue of named person warrants for investigation of Class 1 and Class 2 offences were also in dispute. The Criminal Law Committee of the Law Society of New South Wales ('the Law Society') stated that the test in proposed paragraph 45A(e)(i) (in relation to Class 1 offences) and paragraph 46A(2)(d) (in relation to Class 2 offences) simply required the issuing authority to have regard to the extent to which methods of investigation not involving named person warrants have been used or are available.[18] A similar point was made by the Privacy Commissioner.[19] The Law Society claimed that the issuing authority should be required to be satisfied in both cases that methods of investigation not involving

---

11 *Transcript of evidence*, New South Wales Police Service, p.16.

12 *Submission No 2*, Independent Commission against Corruption, p. 2.

13 The US Department of Justice and the FBI had stated that the bulk of warrant applications still related to particular services, *Transcript of evidence*, Attorney-General's Department, p. 6

14 *Transcript of evidence*, Attorney-General's Department, pp. 6-7.

15 *Transcript of evidence*, Victoria Police, p. 23.

16 *Transcript of evidence*, Victoria Police, p. 22.

17 *Transcript of evidence*, New South Wales Police Service, p. 24.

18 *Submission No 9*, Criminal Law Committee, Law Society of New South Wales, p. 2.

19 *Submission No.8*, Privacy Commissioner, p. 2.

named person warrants were entirely inappropriate or had been used and had proved to be entirely insufficient.

2.11 These assertions fail to take account of the difference already existing in the Principal Act between the provisions relating to Class 1 and Class 2 offences. The Committee reads proposed section 45A as following the current section 45. It requires the issuing authority to be satisfied, having regard to the extent to which other methods have been used or are available, that the information to be obtained from a named person warrant cannot appropriately be obtained from such other methods.

2.12 On the other hand, the Committee acknowledges that the Law Society and the Privacy Commissioner have correctly stated the impact of proposed paragraph 46A(2)(d), which (like the current section 46) requires the issuing authority, having regard to the extent to which other methods have been used by, or are available to, the agency, to be satisfied that he or she should issue a warrant. The Law Society also suggested that the privacy clause in proposed 46A(2)(a)[20] be also inserted in proposed sections 11B[21] and 45A.

2.13 As indicated, the provisions of the Bill follow the pattern already established in the Principal Act. Section 45, proposed section 45A, section 46 and proposed section 46A all require the issuing authority to have regard to the extent to which other methods have been used by, or are available to, the agency. However, section 45 and proposed section 45A also require the issuing authority to be satisfied that some or all of the information to be obtained through interception could not appropriately be obtained by other methods. On the other hand, section 46 and proposed section 46A merely require the issuing authority to be satisfied that he or she should issue a warrant. Again section 46 and proposed section 46A have privacy clauses whereas sections 11A (enabling ASIO to obtain foreign intelligence from a particular service) and proposed section 11B, section 45 and proposed section 45A do not.

2.14 Addressing the matter of privacy clauses, the Attorney-General's department confirmed that distinctions had been consciously drawn in the Principal Act between the various matters for which warrants could be obtained:

> They (the Law Society) next make a point on privacy, arguing that the present privacy provisions are inadequate because they only apply to in relation to class 2 offences and not class 1. That dates back to inquiries made by a parliamentary committee where distinctions were made between class 1 and class 2 offences. For present purposes, we are incorporating that privacy test in relation to named person warrants.[22]

2.15 The Committee does not read the submission of the Law Society as directed at the present privacy provisions but only at their application to the Bill. Whichever way it is to be read, the point remains that insufficient material has been put before the Committee to persuade it to recommend that the Bill should deviate from the patterns already established in the Principal Act, or that those patterns should be overturned.

---

20 That is, the issuing authority to have regard to the likely interference of a named person warrant with any person's privacy

21 That is, named person warrants for collection of foreign intelligence by ASIO.

22 *Transcript of evidence*, Attorney-General's Department, p. 10

Restricting the number of services intercepted under named person warrants

2.16 There was obvious concern at the freedom which named person warrants appeared to give user-agencies. The Law Society claimed that the proposal could lead to an unlimited number of services being intercepted. The Western Australian Police Service argued that rather than an agency having internal arrangements under which, say, its chief officer could add new services to any specified in the original warrant, it would be better if the legislation gave the issuing officer this function on a telephone application. The Privacy Commissioner suggested that the Bill should include procedures for providing independent, effective supervision of the operation of named person warrants in relation to services not identified in the warrants:

- each new interception should be reported to the issuing authority as soon as practicable;
- the report should set out the basis for identifying the service as one that the person named in the warrant is using or is likely to use;
- the issuing authority may require the interception of the new service to cease if there are insufficient grounds for it to continue.[23]

2.17 Specific arguments against the suggestion of the Western Australian Police Service that the issuing authority permit the inclusion of previously unspecified services on a warrant by telephone were put by the Victoria Police. These indicated that the availability of AAT members to hear an application can be a factor in delays in the issue of warrants.[24] The ICAC also stated that in a fast-moving situation it may be difficult, if not impossible, to contact the person who issued the warrant,[25] in order to have the service added to the warrant.[26] Insofar as the suggestion of the Privacy Commissioner involves procedures after the event, it has the obvious advantage of not preventing the agency concerned from changing quickly to new services. On the other hand, the ICAC argued against such an approach because it would involve a *prima facie* illegal intercept until such time as approval was granted.[27]

2.18 In any case, it appears that the apparent freedom given to user-agencies to intercept services at will is to be restrained by their obligation to report under proposed section 94B and the existing liability to inspection. Proposed section 94B will require an agency to which a named person warrant has been issued to report to the Minister within 3 months after the warrant ceases to be in force. The report is to contain the following information about each interception made under the warrant:

- The service to or from which the intercepted communication was made (being a service that the person named in the warrant used, or was likely to use);

---

23 *Submission No*. 8, Federal Privacy Commissioner, p.4

24 *Submission No 3*, Victoria Police, page 5.

25 Or other persons

26 *Submission No. 2*, Independent Commission against Corruption, pages 2-3.

27 *Submission No. 2*, Independent Commission against Corruption, page 3.

- The reasons it would not have been effective to intercept the communications under a telecommunications service warrant;
- The use made by the agency of information obtained by each interception;
- Information about the communication of such information to persons outside the agency;
- The number of arrests made, or likely to be made, on the basis of such information;
- An assessment of the usefulness of information obtained by each interception.

2.19 The Attorney-General's department commented specifically on some of these matters, in particular the first suggestion of the Privacy Commissioner:[28]

> We have already got provisions in there that require a kind of ex post facto justification of what the law enforcement agency has done through their listing the services intercepted and reporting on what was gathered from that interception and the extent to which it assisted the investigation – in other words, so that the inspecting agency, be it the Ombudsman or a state Ombudsman or whoever can consider whether this was within the intent of the legislation, can report on it. [29]

2.20 The Attorney-General's department officer noted of the second suggestion made by the Privacy Commissioner that he believed it to be incorporated in the Bill.[30] The Committee suggests that he was probably referring to the fact that if one relates all the intercepted communications to the services involved, one can readily judge whether the person named in the warrant used, or was likely to use, them. Of the Privacy Commissioner's concerns he stated:

> I think that is there in the bill now, perhaps not explicitly but certainly encompassed in the intent of it. If the Ombudsman, for example, were to note that . . . when action shifted to another person, that interception just continued on that service, even though the suspect had moved onto another one, the obvious question is why? . . . I do not think you can provide for hard and fast copper bottom guarantees in this area but, to the extent that you can provide for accountability, we have encompassed that through this measure.[31]

2.21 The Committee is not satisfied that a case has been made out for replacement of the proposed provision for ex post facto reporting to the Minister on interceptions under named person warrants, particularly when combined with the inspecting role of the various Ombudsmen. It seems to the Committee that, even if a system of reporting back to the issuing authority was adopted, the proposed provision for reporting to the Minister would still be necessary.

---

28 The comment is also relevant to the concern expressed by the Law Society and the suggestion of the Western Australian Police Service.

29 *Transcript of evidence*, Attorney-General's Department, p. 4.

30 *Transcript of evidenc*e, Attorney-General's Department, pages 4-5.

31 *Transcript of evidence*, Attorney-General's Department, p. 5.

Use of intercepted information

2.22 The Principal Act permits information obtained by intercept to be given in evidence in certain proceedings (called 'exempt proceedings'). The Court of Appeal of New South Wales ruled by majority in the case of Wood v Beves[32] that such information could not be given in subsequent proceedings. Proposed section 75A[33] would overcome the effect of that decision by permitting information obtained by intercept and given in evidence in an exempt proceeding to be given later in any proceeding.

2.23 The Law Society opposed the amendment. It believed that it would sound the death knell of the exempt proceedings limitations, already consisting of 14 categories and that it should be limited to the facts of Wood v Beves, and simply name contempt proceedings as a new exempt proceeding. The Committee considers that it would still be necessary for intercepted information to be used in exempt proceedings before it could be used in other proceedings. The Committee considers that the proposed amendment in the Bill is more logical than that suggested by the Law Society and in keeping with the view expressed in the minority decision in Wood v Beves.[34]

2.24 On the other hand, the Committee is inclined to the view that the consequences predicted by the Law Society *could* occur if a suggestion of the New South Wales Police Service was adopted. This supported the inclusion of proposed section 75A, but argued that it should be extended to enable the product of telecommunication intercept to be used in specific circumstances involving the health, welfare or safety of people. However, the representative of the New South Wales Police appeared to agree that it would be impossible for the Committee to recommend that an intercepting agency be allowed to pass intercept material in the interests of such broad categories as 'health, welfare or safety of people'.[35]

2.25 The Committee notes that in evidence the Attorney-General's department agreed that the provision would be subject to the general rules of admissibility so that the rights of the accused and the proper trial process would still have to be observed.[36] The Committee suggests that the Attorney-General consider the insertion of a note to that effect in the Bill.

Recommendation 2

The Committee **recommends** that a note be inserted in the Bill to make it quite clear that proposed section 75A is subject to the general rules of admissibility.

32 (1997) 137 FLR 436

33 See item 58 of Schedule 3, Part 1

34 Handley JA, (1997) 137 FLR 436, at pp. 439-442. He argued that by authorising the use of lawfully obtained information in evidence in an exempt proceeding, the Principal Act by necessary implication authorises its further use free from restrictions imposed by the Act.

35 *Transcript of evidence*, p. 15.

36 *Transcript of evidence*, Attorney-General's Department, p. 8.

Destruction of extraneous intercepted information

2.26 The Privacy Commissioner also suggested that information intercepted by a law enforcement agency that relates to third parties and not to the agency's legitimate law enforcement activities[37] or information intercepted by ASIO that is not relevant to national security or foreign intelligence purposes[38] be destroyed as soon as practicable or within 6 months of the expiry of the warrant in question. The Attorney-General's department argued against the need for such a provision in the case of Commonwealth law enforcement agencies:

> in the context of an inspection arrangement by the Ombudsman so that, if an agency were keeping material beyond a reasonable time, you would expect that to surface through the accountability arrangements.[39]

2.27 The department also argued that such a provision might introduce an element of inflexibility when the circumstances could vary widely.[40] Commissioner Palmer of the Australian Federal Police illustrated the department's general assertion on inflexibility very graphically:

> The totality of the conversation is obviously important in the context of the trial process. The reality is that many of the conversations are coded conversations. Frequently, you are not sure what you are listening to until the investigation completely unfolds, so you are not really certain as the investigation is unfolding which conversations are suspicious and which are not. . .
>
> Secondly, to interfere and start to be selective about what you keep and what you throw away before an appeal process is completed is enormously dangerous from both a prosecution and an appeal point of view and counterproductive from a defence point of view. They would very quickly argue that we had made a mistake in our decision as to what we should keep and what we should not. To destroy it before the appeal process is completed is not an option open to us, in my view. We still have in our keeping product of several years duration because the appeal process is still running. It is destroyed once the appeal process is run.[41]

---

37 *Submission No 8*, Federal Privacy Commissioner, p. 4.

38 *Submission No 8*, Federal Privacy Commissioner, p. 5.

39 *Transcript of evidence*, Attorney-General's Department, p. 5

40 *Transcript of evidence*, Attorney-General's Department, page 5.

41 *Transcript of evidence*, Australian Federal Police, p. 5. Commissioner Palmer continued: 'It is, though, open to defence and has been run as a defence that conversations we believed to be innocent and unconnected with the suspicious conversations not only were relevant but went to prove that what we thought they were referring to was not what they were referring to. In other words, the connotation we were trying to put on conversations - in terms of 'salt' meaning heroin, for example, - was not right when you listened to the entire conversations. From an evidentiary point of view, it is important to both sides that whatever we keep is kept in total. From our point of view, it would be a mistake for us to destroy it before the full appeal process is run, and you certainly could not guarantee that around a six-month or arbitrary limit, or whatever it was. But we should have an obligation to destroy it the moment that appeal process has run, which is what we do.

2.28 Mr Richardson, Director-General of Security, indicated that ASIO was strictly accountable[42] :

> . . . we at ASIO have – and properly so – a very tight accountability arrangement around us, overseen by the Inspector-general of Intelligence and Security, who is a separate statutory appointee reporting to the Prime Minister. …it is a statutory authority which does not require the approval of government in order to initiate a particular inquiry in respect of us. That office has complete access to any information which we hold at any point, and part of their responsibility is to ensure that our warrants are conducted lawfully and that the destruction of material is done in accordance with the law, et cetera.[43]

2.29 The Attorney-General's department indicated that similar accountability arrangements applied to State law enforcement agencies:

> The first point is on the interaction between the federal legislation and state legislation. The essential point is that the federal act marks out the high ground, if I can put it in those terms: it declares what needs to be done by a state if a state agency is to be granted the power to intercept, bearing in mind that the federal parliament has competency in this area because telecommunications is a federal concern. Section 35 of the Act sets out a whole range of matters which must be satisfied by state legislation in relation to a state police force or a state law enforcement agency before that agency can be declared by the Attorney. Perhaps the most significant is paragraph (h) of section 35 (1) which deals with the inspection arrangements by an independent authority, such as an ombudsman or that sort of thing.[44]

Entry onto premises in connection with telecommunications interception

2.30 The Bill provides, by Item 42 in Part 1 of Schedule 3, for deletion of the provision which requires warrants under section 48 authorising entry onto premises as well as interception, to be executed by officers of the Australian Federal Police. There was greater disagreement about the continued need for a provision authorising entry for the purposes of interception than there was about the people who should act under it.[45] The Victoria Police stated that it has never sought a section 48 warrant (for entry on premises), that the need for it has been extremely rare, that changing technology has largely made this type of interception redundant and that the proposed amendment will not impact on its investigative methods.[46]

2.31 On the other hand, the ICAC submission stated that such warrants are important because of PABX systems.[47] In addition, the Review accepts the view of the Australian

---

42 See above, Paragraph 2.25 – the argument put by the Attorney-General's department in relation to Commonwealth law enforcement agencies would also be applicable to it.

43 *Transcript of evidence*, Australian Security Intelligence Organisation, page 6.

44 *Transcript of evidence*, Attorney-General's Department, page 25.

45 The Law Society did suggest that there appears to be no requirement for the premises to be entered under section 48 to be named in connection with a named person warrant. However, proposed subsections 9A and 11B and subsections 48(1), (2) and (3) require the premises to be specified.

46 *Submission No. 3*, Victoria Police, page 5.

47 *Submission No. 2*, Independent Commission against Corruption, page 4.

Federal Police that the growth of 'virtual private networks' will require an on-site interception capability, as communications in large entities are increasingly being encrypted and carried as data, not as voice.[48] In the circumstances, although the issue was not examined closely, it appears to the Committee that continuation of the existence of the warrant for entry is justified.

The adequacy of reporting mechanisms

2.32 As indicated above, the reporting mechanisms provided for in the Bill (and the Principal Act) will play a crucial role in ensuring that named person warrants are not abused. However, submissions did not focus on their adequacy as such. The Committee is able to say that, on examination, they appear adequate. However, it will be helpful to have a review mechanism in place to examine them in practice.

48 Telecommunications Interception Policy Review, paragraphs 7.4.10-11.

APPENDIX 1

ORGANISATIONS THAT PROVIDED THE COMMITTEE WITH SUBMISSIONS

Organisation	Sub. No.
Telecommunications Interceptions Branch, New South Wales Police Service	1A
Independent Commission Against Corruption	2
Victoria Police	3
Bureau of Criminal Intelligence	4
National Crime Authority	5
Information and Security Law Division, Commonwealth Attorney-General's Department	6
Information and Security Law Division, Commonwealth Attorney-General's Department	6A
Australian Federal Police	7
Federal Privacy Commissioner	8
Criminal Law Committee, Law Society of New South Wales	9

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Public Hearing, Thursday 27 April 2000 (Sydney)

Mr James Bennett, *National Crime Authority*

Mr Peter Ford, *Information and Security Law Division, Commonwealth Attorney-General's Department*

Dr Michael Palmer, *Australian Federal Police*

Mr Dennis Richardson, *Australian Security Intelligence Organisation*

Detective Chief Inspector Arthur Kopsias, *Telecommunications Interceptions Branch, New South Wales Police Service*

Detective Acting Inspector Gary Manson, *Special Projects Unit, Victoria Police*