THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

Parliamentary Joint Committee on the
Australian Security Intelligence Organization

AN ADVISORY REPORT ON THE AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION LEGISLATION AMENDMENT BILL 1999

May 1999

ISBN

CONTENTS

COMMITTEE MEMBERS

The Hon David Jull MP (Presiding Member)
Mr John Forrest MP
Mr Stewart McArthur MP
The Hon Leo McLeay MP
Senator Sandy Macdonald
Senator David MacGibbon
Senator the Hon Robert Ray

Secretariat

Grant Harrison (Secretary)
Cheryl Scarlett
Jon Bonnar
Cathy Coote

RECOMMENDATIONS

Membership of the Parliamentary Joint Committee on ASIO

The ASIO Legislation Amendment Bill 1999 should contain an additional item repealing subsection 92B(7)(d), so as to allow the Deputy President of the Senate and the Deputy Speaker of the House of Representatives to be eligible for appointment to the Parliamentary Joint Committee on ASIO. (paragraph 2.28)

Test for issuing a warrant (schedule 1, item 16)

The Attorney-General should issue a supplementary explanatory memorandum for the ASIO Legislation Amendment Bill 1999, clarifying the purpose and intent of Item 16, subsection 25(2). The supplementary explanatory memorandum should make it clear that the provision is not intended to change the test to be applied by the Attorney-General in issuing a search warrant. (paragraph 3.27)

Adding, deleting or altering data (schedule 1, item 16)

The Attorney-General should consider whether an alternative form of words in Item 16, subsections 25(4) and (5) is needed to make it clear that the Bill does not allow ASIO to add, delete or alter data stored in a target computer, except for the purposes of gaining access to the computer.

If the Attorney-General receives advice that the wording of the Bill is adequate for this purpose, a supplementary explanatory memorandum should be issued to explain more clearly the intent of the Bill. (paragraph 3.57)

Recovery of listening and tracking devices (schedule 1, items 22 and 23)

The Inspector-General of Intelligence and Security should report annually to the Attorney-General and the Leader of the Opposition on the frequency with which ASIO recovers listening and tracking devices outside normal warrant periods. (paragraph 3.68)

Memorandum of understanding between ASIO and AUSTRAC (schedule 4, item 1)

Any memorandum of understanding negotiated between the Director of AUSTRAC and the Director-General of Security on access to and use of financial transaction reports information, and any revisions or modifications to such memoranda, should be presented to the Parliamentary Joint Committee on ASIO for consideration before coming into effect. (paragraph 5.33)

Memorandum of understanding between the Inspector-General and AUSTRAC (schedule 4, item 1)

Any memorandum of understanding negotiated between the Director of AUSTRAC and the Inspector-General of Intelligence and Security, and any revisions or modifications to such memoranda, should be referred to the Parliamentary Joint Committee on ASIO for consideration before coming into effect. (paragraph 5.35)

Reporting of access to financial transaction reports information

The ASIO Legislation Amendment Bill 1999 should be amended to include an amendment to the *Financial Transactions Reports Act 1988* requiring the Director of AUSTRAC to include, in AUSTRAC's annual report, information on:

(a) the number of occasions on which ASIO officers interrogated the AUSTRAC database;
(b) the number of occasions on which the Director-General of Security requested access to information on parameters wider than those available through ASIO's authorised online access; and
(c) the number of occasions on which the access requests described at (b) above were granted. (paragraph 6.20)

Memorandum of understanding between ASIO and the Commissioner of Taxation (schedule 6)

Any memorandum of understanding negotiated between the Commissioner of Taxation and the Director-General of Security on access to and use of tax information, and any revisions or modifications to such memoranda, should be presented to the Parliamentary Joint Committee on ASIO for consideration before coming into effect. (paragraph 7.32)

CHAPTER 1

INTRODUCTION

Referral of the Bill to the Committee

1.1 The Attorney-General introduced the Australian Security Intelligence Organisation Legislation Amendment Bill 1999 (the Bill) into the House of Representatives on 25 March 1999. After the Attorney's second reading speech, debate on the Bill was adjourned.

1.2 On 13 April 1999, the Attorney-General wrote to the Presiding Member of the Parliamentary Joint Committee on the Australian Security Intelligence Organization asking that the Committee review the Bill and report back to him by 8 May 1999. A copy of the Attorney-General's letter of referral is at Appendix 1. The conduct of our review is described in Appendix 2.

Purpose of the Bill

1.3 The Australian Security Intelligence Organization (ASIO) is responsible for protecting Australia and its people from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on our defence system and acts of foreign interference.

1.4 ASIO derives its authority from the *Australian Security Intelligence Organization Act 1979* (the ASIO Act). The Bill is directed at ensuring that ASIO remains capable of providing timely intelligence and security advice to governments.

1.5 The Bill proposes to:

- allow ASIO to use contemporary surveillance technologies;
- allow ASIO to access tax and financial information relevant to its investigations;
- improve inter-government administrative arrangements for processing security clearances for the Year 2000 Olympic Games;

- change the provisions in relation to emergency warrants and the duration of search warrants;

- correct anomalies such as the inability to remove a listening device outside the warrant period or to collect foreign intelligence in Australia through the use of human resources; and

- make miscellaneous amendments such as the issue of cost recovery and providing the Australian Federal Police with intelligence obtained from ASIO's international liaison partners.[1]

1.6 The Bill attempts a careful balance of public and private interests. On the one hand there is a clear public interest ensuring that ASIO is adequately and appropriately equipped to safeguard Australia against threats to security. Equally, however, it is important that the activities of ASIO do not threaten individual rights and liberties.[2]

1.7 In his second reading speech the Attorney-General observed that the Bill is not:

> … a response to the challenges posed by a particular event or threat, such as the Olympic Games, notwithstanding that ASIO will have an important role to play in ensuring the safety of athletes, officials and spectators … rather the Bill results from a considered examination of ASIO's capacity to meet its ongoing responsibilities to government in a rapidly changing information environment.[3]

1.8 The Bill proposes changes of substance to the ASIO Act, the *Financial Transactions Reports Act 1988*, the *Taxation Administration Act 1953* and the *Inspector-General of Intelligence and Security Act 1986*, and consequential and minor amendments to numerous other Acts.

Structure of the report

1.9 Chapter 2 of the report will address two general issues: the time available for our review of the Bill and the privacy impact of the Bill.

1.10 Chapters 3 to 7 address the major issues arising in each of the schedules to the Bill:

---

1 Dennis Richardson (Australian Security Intelligence Organization) *Transcript of Evidence*, 27 April 1999, pp. 2-3

2 Attorney-General's Department, *Submission No. 9*, p. 2

3 Hon Daryl Williams AM QC MP (Attorney-General), *House of Representatives Hansard*, 25 March 1999, p.. 4364

- chapter 3 focuses on issues arising from schedule 1, dealing with warrant provisions;
- chapter 4 describes the changes arising from schedules 2 and 3 in relation to penalty provisions and the change to the spelling of the word 'Organization' respectively;
- chapter 5 comments on issues arising from the amendments, in schedule 4, to the *Financial Transaction Reports Act 1988*;
- chapter 6 discusses the amendments to the *Inspector-General of Intelligence and Security Act 1986*; and
- chapter 7 focuses on issues arising from the amendments, in schedule 6, to the *Taxation Administration Act 1953*.

1.11 These chapters provide an overview of the main issues that arose in our review. A number of other issues raised in submissions are tabulated in Appendix 3.

CHAPTER 2

GENERAL ISSUES

Time available to review the Bill

Concerns about the timeframe

2.1 The Bill was referred to us on 13 April 1999, with a reporting deadline of 8 May 1999. This gave us three and a half weeks in which to conduct our review.

2.2 Complaints about the lack of time available to properly review the Bill were a constant theme in the submissions we received from non-government organisations. In fact, most non-government organisations we contacted were unable to make a submission in the time available and only one of those we invited was able to attend our public hearing on 27 April 1999.

Committee comments

2.3 The Government has not explained the urgency it has attached to our consideration of the Bill.

2.4 We accept that some provisions in the Bill refer to security assessment procedures that need to be in place for the Year 2000 Olympic Games and understand the Government's desire for the Bill to be considered by Parliament as soon as possible.[1]

2.5 Furthermore, we note the remarks by the Director-General of Security that he believes it is important that 'those amendments which the Parliament agrees to are in place before the end of the year'.[2]

---

1 The submission from the Attorney-General's Department contained the following advice: 'One important change [in the Bill] is connected to the Year 2000 Olympic Games. However, as many of the changes concern intelligence collection, the Government considers it would be prudent for Australia to have them in place before the Olympics. The Government has given a high priority to the Bill and wishes it to be considered by Parliament as soon as possible.' (Attorney-General's Department, *Submission No. 9*, p. 2)

2 Dennis Richardson (Australian Security and Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 5

2.6 Nevertheless, it is unfortunate that we have had such a brief period in which to review the Bill. As a consequence, some people who wanted to contribute have not been able to and others have speculated that the tight timeframe has been imposed so as to limit public and parliamentary scrutiny of the Bill.

2.7 We do not believe that the timeframe was imposed with this intent, but the suspicion could have been avoided if a more reasonable timeframe had been allowed.

2.8 Notwithstanding these concerns, it is important to acknowledge that the objectives contained in the Bill have already been the subject of extensive consultation, both within government,[3] and between the Australian Transactions Reports and Analysis Centre (AUSTRAC) and a wide range of parties with an interest in financial, privacy and civil liberties matters.[4]

2.9 We have been advised that these consultations, particularly those conducted by AUSTRAC in relation to ASIO's access to financial transaction reports information, were influential in determining the nature of the provisions in the Bill and the operational arrangements giving effect to the Bill.[5]

---

3 See the Director-General's advice that 'the amendments have been developed over two years of consultation between the Australian Security Intelligence Organization, Inspector-General of Intelligence and Security, Attorney-General's Department, Australian Transaction Reports and Analysis Centre, Australian Taxation Office, Department of Prime Minister and Cabinet, Department of Foreign Affairs and Trade, the Department of Treasury, Department of Defence and other members of the Australian intelligence community.' (Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 4

4 Those involved in AUSTRAC's consultations (which focussed on ASIO's access to financial transaction reports information) included the Australian Bankers Association; Australian Finance Conference; Colonial State Bank Limited; Commonwealth Bank; Credit Union Services Corporation of Australia Limited; National Australia Bank; Reserve Bank; St George Bank; Chase Manhattan Bank; Westpac Bank; Australian Association of Permanent Building Society; ANZ Bank; Victorian Council of Civil Liberties, Privacy Commissioner, and the Electronic Money Information Centre. (Australian Transaction Reports and Analysis Centre, *Submission No. 7*, p. 13)

5 See the advice from the Director of AUSTRAC that 'AUSTRAC believes that the measures contained in the memorandum of understanding [between ASIO and the Inspector-General of Intelligence and Security] … address the concerns of both AUSTRAC and its Provider Advisory Group and Privacy Committee insofar as these relate to administrative arrangements.' (Australian Transaction Reports and Analysis Centre, *Submission No. 7*, p. 19). See also the comments in a second submission from AUSTRAC indicating that the Australian Finance Conference is supportive of the terms of the memorandum of understanding (Australian Transaction Reports and Analysis Centre, *Submission No.15*, p. 1).

2.10 Finally, we note that the Bill will be subject to further debate and consideration in the Parliament. This may provide an opportunity for further public submissions to be taken.

Privacy impact of the Bill

Concerns raised in evidence

2.11 Another common theme in submissions from non-government organisations was concern about the privacy impact of the Bill.

2.12 Organisations such as the Australian Privacy Charter Council, Privacy New South Wales and Electronic Frontiers Australia acknowledged the need to protect Australia's security and intelligence interests, but expressed concern that the expanded surveillance and information gathering powers could result in unreasonable intrusions in the personal affairs of Australian citizens.[6]

2.13 The Privacy Charter Council drew our attention to the Australian Privacy Charter Principles, a statement of best practice for the protection of privacy, which refers to the need to ensure fair handling of personal information and minimal levels of surveillance of Australians in their daily activities.[7] The Council suggests that adherence to these principles is a minimum requirement for ASIO.

2.14 Privacy New South Wales likewise argues for the importance of privacy protections and adequate accountability arrangements to ensure that 'peoples' reasonable expectations of privacy' are not undermined.[8]

2.15 Electronic Frontiers Australia submitted that:

> While keeping law-enforcement and intelligence-gathering agencies relevant to the digital age is a worthy aspiration, it should be remembered that computer technology has the capacity to monitor individuals and damage an individual's reputation in ways not possible in times past. It is important that the use of technology be restrained by reference to rights of privacy guaranteed under the

6 See Australian Privacy Charter Council, *Submission No. 2*; Privacy New South Wales, *Submission No. 5*; and Electronic Frontiers Australia, *Submission No. 10*

7 Australian Privacy Charter Council, *Submission No. 2*, p. 1

8 Privacy New South Wales, *Submission No. 5*, p. 1

> United Nations Declaration of Human Rights and traditional review of the actions of the Executive by the Courts.[9]

2.16 These, and similar sentiments, were also present in submissions from Joan Coxsedge, the Australian Taxation Institute, the Financial Services Consumer Policy Centre and the Australian Council for Civil Liberties. They also underpin a number of the concerns raised in relation to particular provisions of the Bill which are discussed elsewhere in the report.

Government responses

2.17 When presenting the Bill to Parliament the Attorney-General referred to the difficulty in achieving a balance between the rights of individuals and the preservation of national security.[10]

2.18 The Inspector-General of Intelligence and Security, in his written submission, recognised that while it is important that ASIO 'move with the times' it must not do so:

> … at the cost of an unreasonable diminution of the freedoms which all Australians have come to expect and enjoy.[11]

2.19 The privacy framework within which ASIO operates was described to us by the Attorney-General's Department in the following terms:

> While the *Privacy Act 1988* does not apply to ASIO, the Attorney-General has issued guidelines under section 8A of the ASIO Act dealing with the treatment of personal information by the Organization.
>
> As the Bill will allow ASIO to access additional forms of personal information for the performance of its functions, the Attorney-General has decided that the present guidelines should be reviewed in consultation with the Privacy Commissioner.[12]

---

9 Electronic Frontiers Australia, *Submission No. 10*, p. 1

10 Hon Daryl Williams AM QC MP (Attorney-General), *House of Representatives Hansard*, 25 March 1999, p. 4364

11 Inspector-General of Intelligence and Security, *Submission No. 1*, p. 2

12 Attorney-General's Department, *Submission No. 9*, p. 12

2.20 The review will be conducted before the Bill is enacted and the revised guidelines will be tabled in Parliament in accordance with subsection 8A(4) of the ASIO Act.[13]

2.21 The Attorney-General's Department also noted that the Privacy Commissioner (after assessing the controls governing ASIO's access to financial transaction reports information and tax information, and the monitoring functions of the Inspector-General of Security and Intelligence) had reported that his concerns about the new data flows becoming entrenched without independent scrutiny 'should be substantially allayed'.[14]

Committee comments

2.22 We concur with many of the views expressed on the importance of privacy safeguards:

- we agree that expanded surveillance and information gathering powers should not result in unreasonable intrusions in the personal affairs of Australian citizens;
- we agree that privacy protections must ensure the fair handling of personal information and levels of surveillance consistent with operational needs, but no more; and
- we agree that privacy protections must recognise that modern surveillance techniques can, if misused, damage an individual's reputation in ways not possible in the past.

2.23 We note that the Privacy Commissioner has reviewed and accepted, in general terms, the privacy framework described in the Bill and that he is to participate in a review of the privacy guidelines issued by the Attorney-General to ASIO.

2.24 We look forward to the tabling in Parliament of the Attorney-General's revised privacy guidelines.

13 Attorney-General's Department, *Submission No. 9*, p. 12

14 Attorney-General's Department, *Submission No. 9*, p. 13

Membership of the Parliamentary Joint Committee on ASIO

2.25 We take the opportunity afforded by this review to suggest that an anomaly in relation to the membership arrangements for this Committee also be resolved.

2.26 Section 92B(7) of the ASIO Act provides that various people are not eligible for appointment to the Parliamentary Joint Committee on ASIO, including the Deputy President and Chairman of Committees of the Senate and the Chairman of Committees of the House of Representatives.

2.27 Both the Deputy President of the Senate and Chairman of Committees of the House (now known as the Deputy Speaker) serve on other committees of the Parliament and there are no compelling reasons why they should be excluded from serving on the ASIO Committee. Accordingly, we make the following recommendation.

2.28 The ASIO Legislation Amendment Bill 1999 should contain an additional item repealing subsection 92B(7)(d), so as to allow the Deputy President of the Senate and the Deputy Speaker of the House of Representatives to be eligible for appointment to the Parliamentary Joint Committee on ASIO.

CHAPTER 3

SCHEDULE 1 – WARRANT PROVISIONS ETC.

Background

3.1 Schedule 1 contains various amendments to the ASIO Act. This chapter considers the most significant of the issues raised in our evidence on schedule 1.

Item 16, section 25 – Search warrants

3.2 Item 16 repeals the existing section 25 in the ASIO Act and replaces it with a new section 25 dealing with search warrants.

Subsection 25(1) – Issue of search warrant

3.3 Subsection 25(1) allows the Attorney-General, on request of the Director-General of Security and in accordance with the test described in subsection 25(2), to issue a search warrant.

Concerns raised in evidence

3.4 The Australian Council for Civil Liberties argued that a process that allows the Attorney-General to issue warrants is far less accountable than a process which requires law enforcement agencies to seek warrants from judicial authorities.[1]

> For a mainstream law enforcement agency … the justification for the issue of search warrants can and frequently is challenged in the courts as a means of maintaining the balance between police powers and the civil liberties of individuals.[2]

3.5 Submissions from Privacy New South Wales, Electronic Frontiers Australia and the Australian Privacy Charter Council raised similar objections.

---

1 Australian Council for Civil Liberties, *Submission No. 14*, p. 3

2 Australian Council for Civil Liberties, *Submission No. 14*, p. 3

3.6 Privacy New South Wales called for a review of the system of ministerial authorisation of warrants and proposed a 'more arms length process using judicial officers'.[3] Electronic Frontiers Australia drew attention to the warrant approval procedures in Holland, where three ministers must sign warrants.[4] The Australian Privacy Charter Council suggested that the warrant approval function should rest with 'some independent officer – perhaps one or more retired senior judges nominated by the judiciary.'[5]

Government response

3.7 The Director-General explained the operation of the warrant approval process in his evidence at our public hearing.

> First of all, within ASIO any warrant proposal must be approved within the collection area by the head of that division. Secondly, it must be approved by the legal adviser. Thirdly, the request must be signed by the Director-General personally. It is not an authority which is delegated. Fourthly, any warrant request, after it is signed by the Director-General of Security, goes to the Attorney-General's Department where a separate certificate is signed authorising that the warrant request is consistent with the Act. Finally, warrant requests must be considered and approved by the Attorney-General personally. Again, they are not matters which the Attorney-General can delegate.
>
> Beyond that, the Inspector-General of Intelligence and Security reviews all warrant files on a regular basis[6]

3.8 The Director-General also argued that sections 21 and 94 of the ASIO Act provide an additional check on ASIO's operations, including its warrant applications, by requiring that the Leader of the Opposition in the House of Representatives be regularly consulted on matters relating to security and be provided with a copy of ASIO's classified annual report.[7]

---

3 Privacy New South Wales, *Submission No. 5*, p. 2

4 Electronic Frontiers Australia, *Submission No. 10*, p. 3

5 The Australian Privacy Charter Council, *Submission No. 11*, p. 5. Chris Connolly, from the Financial Services Consumer Policy Centre, referred to this debate in oral evidence (see Chris Connolly (Financial Services Consumer Policy Centre), *Transcript of Evidence*, 27 April 1999, p. 47

6 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, pp. 3-4

7 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, pp. 3-4

Committee comments

3.9 The warrant application and approval processes are clearly different for ASIO than they are for law enforcement agencies. In our view the nature of ASIO's operations justify these differences.

3.10 It would be impractical and inappropriate to adopt any of the alternatives suggested to us in evidence.

3.11 To involve more than one minister in the approval process would cause considerable delays, would involve a diminution of accountability (with no one minister taking responsibility for the ultimate decision), and would risk wider knowledge of the circumstances of the warrant request than is necessary.

3.12 To require ASIO to apply either a retired or current judicial authority, rather than to the Attorney-General, would not make the process any more open or transparent (warrant applications would, of necessity, be heard *in camera*) and would not strengthen accountability (as parliamentarians are subject to a far more rigorous and direct system of accountability than judges or retired judges).

3.13 Finally, we note that in 1997 the judges of the Federal Court advised the Government that they would no longer be involved in issuing telecommunication interception warrants. The judges advanced three reasons for their decision:

- issuing warrants is an administrative, not a judicial function;
- issuing warrants imposes a significant additional workload; and
- they were increasingly finding themselves as respondents to judicial review applications in their own courts.[8]

8 See Hon Daryl Williams AM QC MP (Attorney-General), *House of Representatives Hansard*, 27 August 1997, p. 7089. As a result, Parliament enacted the *Telecommunications (Interception) and Listening Device Amendment Act 1997*, the effect of which, in part, was to authorise members of the Administrative Appeals Tribunal to issue telecommunications interception and listening device warrants under the *Australian Federal Police Act 1979* and the *Customs Act 1901*.

Subsection 25(2) – Test for issue of warrant

3.14 According to the explanatory memorandum for the Bill, subsection 25(2) simplifies the description of the matters about which the Attorney-General must be satisfied before issuing a warrant.

3.15 The existing provision in the ASIO Act reads as follows:

> Where … the Minister is satisfied that there are reasonable grounds for believing that there are in any premises any records or other things without access to which by ASIO the collection of intelligence by ASIO in accordance with this Act in respect of a matter that is important in relation to security would be seriously impaired, the Minister may [issue a warrant].

3.16 The proposed new subsection 25(2) allows the Attorney-General to issue a warrant if he or she is satisfied that 'access to the records or other things on particular premises will substantially assist the collection of intelligence in a matter that is important in relation to security.'

Concerns raised in evidence

3.17 We received a number of submissions objecting to subsection 25(2) on the grounds that it significantly relaxed the test to be applied by the Attorney-General in deciding whether to issue a warrant.

3.18 Chris Connolly, on behalf of the Financial Services Consumer Policy Centre, argued that the test contained in the existing Act required the Attorney-General to be satisfied in relation to four matters before issuing a warrant:[9]

> They are that he must have reasonable grounds for believing that certain material exists on the premises, that ASIO requires access to that material, that the collection of intelligence by ASIO would be seriously impaired without access to that material, and that the above collection is important in relation to security.[10]

3.19 On the other hand, Mr Connolly considered that the proposed new subsection 25(2) simply requires the minister be satisfied that there are reasonable grounds for believing that the information will substantially assist the collection of intelligence in accordance with the ASIO Act. This

---

9 Chris Connolly (Financial Services Consumer Policy Centre), *Transcript of Evidence*, 27 April 1999, p. 39

10 Chris Connolly (Financial Services Consumer Policy Centre), *Transcript of Evidence*, 27 April 1999, p. 39

changes the test from a negative test in which ASIO has to be obstructed in its duties before a warrant will be issued to a test that just says that ASIO must be assisted.[11]

3.20 Mr Connolly also made the point that the question of whether the test was intentionally being change by the amendment was not addressed in either the explanatory memorandum for the Bill, the Attorney-General's second reading speech, or the submission from the Attorney-General's Department.[12]

3.21 A number of other organisations supported Mr Connolly's concerns.[13]

Government response

3.22 The submission from the Attorney-General's Department explained that the purpose of the new subsection 25(2) is to make the current provision 'more comprehensible by stating the test in a positive rather than a negative form.'[14]

3.23 In evidence at our hearing, Norman Reaburn, on behalf of the Attorney-General's Department, and the Director-General of Security addressed this issue by saying:

> We believe that the test is a test of similar import. In that sense, what we have done is simplify the way in which the thing is proposed (Mr Reaburn)
>
> … the driving force behind this amendment … was to use plain English language to the extent possible. It was not to lower the test. (Mr Richardson).[15]

---

11 Chris Connolly (Financial Services Consumer Policy Centre), *Transcript of Evidence*, 27 April 1999, p. 39

12 Chris Connolly (Financial Services Consumer Policy Centre), *Transcript of Evidence*, 27 April 1999, p. 39

13 See Electronic Frontiers Australia, *Submission No. 10*, p. 3; The Australian Privacy Charter Council, *Submission No. 11*, p. 4; and Australian Council for Civil Liberties, *Submission No. 14*, p. 8

14 Attorney-General's Department, *Submission No. 9*, p. 5

15 Norman Reaburn (Attorney-General' Department), *Transcript of Evidence*, 27 April 1999, p. 56; and Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 57

Committee comments

3.24 We note that section 15AC of the *Acts Interpretation Act 1901* provides that changes in style shall not affect the meaning of a provision. This means that where an Act has expressed an idea in a particular form of words and a later amendment changes the wording to present a clearer style, the original ideas are retained.

3.25 This provision will ensure that the test to be applied by the Attorney-General in issuing a warrant will not change, despite the change in wording.

3.26 Nevertheless, we consider that the Government's intention in this matter (to change the words but not the test) could be made clearer. Accordingly, we make the following recommendation.

3.27 The Attorney-General should issue a supplementary explanatory memorandum for the ASIO Legislation Amendment Bill 1999, clarifying the purpose and intent of Item 16, subsection 25(2). The supplementary explanatory memorandum should make it clear that the provision is not intended to change the test to be applied by the Attorney-General in issuing a search warrant.

Subsections 25(8), 25(10) – Delayed commencement and duration of warrants

3.28 Subsection 25(8) proposes to allow the Attorney-General to delay the commencement of a search warrant for up to 28 days after the day on which it is issued. Subsection 25(10) allows the Attorney-General to extend the maximum period in which a search warrant is in force from 7 to 28 days.

Concerns raised in evidence

3.29 The Australian Privacy Charter Council expressed concern that these provisions represented a major increase in ASIO's discretion and a loss of detailed control by the Attorney-General.

> Any such change which makes it easier for ASIO to obtain a warrant, or to use one warrant instead of making separate

> applications, runs the risk of encouraging a less disciplined use of ASIO's powers.[16]

Government response

3.30 As described in the explanatory memorandum, the purpose of these amendments is to give greater flexibility to ASIO. Unlike law enforcement agencies, most search warrants issued to ASIO need to be executed covertly and it may take time for a suitable opportunity to arise.

3.31 This explanation was endorsed by the Director-General in his evidence at our hearing, when he said:

> … the current [warrant duration] period of seven days is too narrow in the sense that targets can vary their intentions and they can make last-minute decisions to do things differently from what we assessed. When that happens, we are required to go back, sometimes at very short notice, and get a second warrant.[17]

3.32 The Director-General acknowledged, however, that ASIO has both an operational interest and an 'obligation' to execute search warrants as soon as possible and, if there is an opportunity to do so, within seven days from the date of the warrant being issued.[18]

3.33 The Attorney-General's Department noted that the amendment allows the Attorney-General to retain control over the circumstances of the warrant. For example, the delayed application provisions would only be given effect in 'circumstances in which the Attorney-General is satisfied that there are grounds for issuing a search warrant in relation to particular premises but the Attorney-General is also satisfied that the warrant cannot be immediately executed'.[19]

3.34 The Attorney-General's Department observed that this problem is not shared by law enforcement agencies which 'generally speaking,

---

16 The Australian Privacy Charter Council, *Submission No. 11*, p. 4. The Australian Council for Civil Liberties and Electronic Frontiers Australia also expressed concern about the extension of the duration of warrants and the delayed application provisions. See Australian Council for Civil Liberties, *Submission No. 14*, pp. 7-8 and Electronic Frontiers Australia, *Submission No. 10*, pp. 3-4

17 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 11

18 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 14

19 Attorney-General's Department, *Submission No. 9*, p. 6

execute search warrants openly in the presence of persons occupying premises being searched'.[20]

3.35 Finally, the Attorney-General noted in his second reading speech that, notwithstanding the provisions allowing an extended warrant period and delayed commencement, a search warrant authorises only one search of a premises.[21]

Committee comments

3.36 While the Bill does allow for an increase in the duration of search warrants and for the commencement of warrants to be delayed, it does not confer discretion on the Director-General in these matters.

3.37 It is the Attorney-General who issues warrants; it is the Attorney-General who considers whether delayed commencement should be allowed; and it is the Attorney-General who decides whether there are sufficient reasons to extend the period of a warrant up to 28 days.

3.38 We accept the need for ASIO to have a greater degree of flexibility in executing warrants than it has at present. We consider that the Bill allows for an appropriate degree of flexibility, while ensuring that ministerial control is retained.

3.39 We note the Director-General's advice that he perceives ASIO's responsibility as being to execute warrants as soon as possible and, if circumstances permit, within seven days of issue. We expect this objective will be written into ASIO's internal operating procedures.

Section 25A – Computer access warrants

3.40 The proposed section 25A will allow the Attorney-General to issue a warrant authorising ASIO to gain remote access to data held in a computer, where such access will substantially assist the collection of intelligence in respect of a matter that is important in relation to security.

---

20 Attorney-General's Department, *Submission No. 9*, p. 6

21 Hon Daryl Williams AM QC MP (Attorney-General), *House of Representatives Hansard*, 25 March 1999, p. 4364. This point was expanded upon in a second submission from the Attorney-General's Department with the statement that the amendment does not 'authorise ASIO to enter premises from time to time during the extended period.' (see Attorney-General's Department, *Submission No. 16*, p. 2)

3.41 The provisions also allow the Attorney-General to authorise ASIO to add, delete or alter data for the purpose of gaining access to data in a target computer and to do things that are reasonably necessary to conceal that anything has been done under the warrant. The explanatory memorandum states that this would include modifying access control and encryption systems.

3.42 However, ASIO is not permitted to obstruct the lawful use of a computer or to anything that causes loss or damage to a person lawfully using the computer or other electronic equipment.[22]

Concerns raised in evidence

3.43 The main concerns raised in evidence about the computer access warrant provisions focussed on subsection 25A(4)(a)(iii) (which allows ASIO to 'add, delete or alter data in the target computer'), and on the relationship between these amendments and the broader community debate about whether law enforcement and intelligence agencies should, by right, have access to keys that decode encrypted data.

3.44 The Australia Privacy Charter Council argued that to allow ASIO to add, delete or alter data would undermine, perhaps fatally, public trust and confidence in the integrity of electronic transactions.[23]

3.45 Electronic Frontiers Australia expressed similar concerns, stating that the Bill appears 'to authorise the covert insertion of material on to a citizen's computer' and that such changes create:

- a risk to business (small changes can have extreme, unforeseen and costly effects);
- a risk of accidental damage to software or data (what redress is available to the owner of the computer if the intrusion was covert and the perpetrator is therefore unknown); and
- a risk of evidence being planted. [24]

3.46 The Financial Services Consumer Policy Centre, while recognising that it is appropriate to allow ASIO to conceal its activities

---

22 See explanatory memorandum for the ASIO Legislation Amendment Bill 1999, pp. 6-7

23 The Australian Privacy Charter Council, *Submission No. 11*, p. 4

24 Electronic Frontiers Australia, *Submission No. 10*, p. 2

under a computer access warrant, submits that this should not extend to altering computer data. The Centre proposes, as an alternative, that references in the Bill to adding, deleting or altering computer data be removed and that ASIO rely on subsection 25(4)(c) (which allows it to do anything necessary to conceal its access) to ensure that its 'tracks are covered'.[25]

3.47 In relation to encryption keys, the Financial Services Consumer Policy Centre expressed grave concern about the way in which the Bill appears to allow ASIO access to the tools for breaking cryptographically encoded data. Chris Connolly argued in his evidence that the Bill does not simply 'tidy-up' the ASIO Act computer access provisions, but:

> … actually delivers and resolves one of today's most controversial and burning issues concerning cryptography and the use of encryption tools by citizens and the balancing of their rights with government rights to gain access to cryptographic keys.[26]

3.48 Mr Connolly suggests that the community debate about whether government agencies should, by right, have access to cryptographic keys should not be resolved by an amendment which allows ASIO to modify access control and encryption systems. He would prefer that these amendments should be withdrawn until such time as the Government develops a 'clear-cut and well articulated policy on cryptography'.[27] The Australia Privacy Charter Council and the Australian Civil Liberties Council supported these concerns.[28]

Government response

3.49 In his second reading speech, the Attorney-General referred to the power to add, delete or alter data when saying that the Bill allows ASIO to do certain things which may be necessary in order to execute a computer access warrant. He stressed, however, that this will be subject to a 'strict limitation that a warrant does not permit ASIO to do anything

---

25 Chris Connolly (Financial Services Consumer Policy Centre), *Transcript of Evidence*, 27 April 1999, p. 41

26 Chris Connolly (Financial Services Consumer Policy Centre), *Transcript of Evidence*, 27 April 1999, p. 40

27 Chris Connolly (Financial Services Consumer Policy Centre), *Transcript of Evidence*, 27 April 1999, p. 40

28 The Australian Privacy Charter Council, *Submission No. 11*, p. 4 and Australian Council for Civil Liberties, *Submission No. 14*, p. 4

that interferes with the lawful use of a computer or causes loss or damage to other persons lawfully using the computer.'[29]

3.50 The extent to which ASIO can 'interfere' with a target computer was explained further by the Director-General in his evidence:

> Under the proposed amendments, we would be allowed to interfere with a computer in so far as it enables us to compromise the protection mechanism that may surround the information in the computer. However, we would not be allowed to interfere with the information in the computer itself or indeed the use of the computer.[30]

3.51 In its written submission the Attorney-General's Department emphasised that that 'in gaining entry to a target computer ASIO is not permitted to cause damage to either computer or data.' it went on to make the point that it would, in fact, be:

> … in ASIO's interests to go to extreme lengths to ensure that it did not cause damage that might compromise its operations.[31]

3.52 At our hearing, both the Director-General and witnesses from the Attorney-General's Department denied that the Bill bore any relationship to the broader debate about government control of encryption keys.

3.53 Norman Reaburn (from the Attorney-General's Department) argued that the debate about whether governments would, at some point in the future, only permit the use of encryption devices to which law enforcement and intelligence agencies have a key is not relevant to this Bill. He concluded that:

> … there is nothing in the current national or international debate that says it is improper for law enforcement and/or security agencies (or other bodies in appropriate circumstances) to be allowed to have, in accordance with the law, access to information which has been encrypted.[32]

---

29 Hon Daryl Williams AM QC MP (Attorney-General), *House of Representatives Hansard*, 25 March 1999 p. 4364

30 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 13

31 Attorney-General's Department, *Submission No. 9*, p. 3

32 Norman Reaburn (Attorney-General's Department), *Transcript of Evidence*, 27 April 1999, p. 58

3.54 The Director-General also sought to distinguish the two issues: stating that the Bill is 'essentially about opening the electronic door to enable us to access data'.[33]

Committee comments

3.55 We believe it is appropriate that the Bill provide for the Attorney-General to authorise ASIO to modify data in a target computer, but only to the extent necessary to gain access to the data stored on the computer.

3.56 Community concerns about government agencies adding to, deleting or altering data stored on personal computers are understandable. These concerns may be allayed if the purpose of the amendments were explained more clearly. Accordingly, we make the following recommendation.

3.57 The Attorney-General should consider whether an alternative form of words in Item 16, subsections 25(4) and (5) is needed to make it clear that the Bill does not allow ASIO to add, delete or alter data stored in a target computer, except for the purposes of gaining access to the computer.

If the Attorney-General receives advice that the wording of the Bill is adequate for this purpose, a supplementary explanatory memorandum should be issued to explain more clearly the intent of the Bill.

3.58 On the basis of the advice we have received, we do not consider that the Bill limits any future options in relation to access to and control of encryption keys.

Item 22, subsection 26(6A) - Recovery of listening devices; and Item 23, subsections 26B(7) and 26C(7) – Recovery of tracking devices

3.59 The proposed subsection 26(6A) will enable ASIO to enter premises to recover a listening device installed under a warrant. ASIO will be able to recovery a listening device while the warrant is in force, or

33 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 58

within 28 days after it ceases to be in force, or at the earliest time practicable after the 28 period.

Concerns raised in evidence

3.60 Joan Coxsedge expressed concern that the recovery arrangements are in effect open ended and that by not fixing a time limit on recovery actions 'the article [or device] could stay put forever or be received when it suits ASIO.'[34] Electronic Frontiers Australia expressed similar concerns, arguing that the power to recover devices should be restricted to the period in which the warrant is in force.[35]

3.61 The Australian Privacy Charter Council stated that the recovery provisions in relation to tracking devices are of particular concern because it will not, in practice, be possible for ASIO to comply with the requirement that tracking devices be deactivated at the expiration of a warrant period.

> By definition, it will be necessary to *use* a tracking device to locate it so that it may be recovered. If ASIO is allowed to delay recovery indefinitely, as is proposed, then this amounts to an indefinite extension of the warrant.[36]

Government responses

3.62 The Attorney-General's Department explained that these provisions are intended to allow ASIO greater flexibility to recover listening and tracking devices undetected.[37] The explanatory memorandum indicates that ASIO is expected to recover a device while the relevant warrant is in force or within the next 28, but makes provision for recovery at the earliest practicable opportunity after that time in situations where a device cannot be retrieved without detection within the specified time periods.

3.63 The explanatory memorandum also notes that the amendment does not authorise ASIO to use a listening device after a warrant has

---

34 Joan Coxsedge, *Submission No. 3*, p. 2

35 Electronic Frontiers Australia, *Submission No. 10*, p. 3. See also the concerns expressed in Australian Council for Civil Liberties, *Submission No. 14*, p. 7

36 The Australian Privacy Charter Council, *Submission No. 11*, pp. 4-5

37 Attorney-General's Department, *Submission No. 9*, p. 5

lapsed or is revoked. The Attorney-General's Department emphasised this point in saying:

> [These amendments] do not in any way extend the period during which ASIO may use a device. As is presently the case, the authority to use a device ends when the warrant expires or it is revoked.[38]

3.64 In response to a question at our hearing on the process for ensuring that listening and tracking devices are deactivated when a warrant expires, the Director-General explained that:

> … all our warrant files are inspected on a regular basis by the Inspector-General of Intelligence and Security. That issue does arise in respect of telecommunications interception also. You have a warrant for six months; someone might change their telephone number. Clearly, we have an obligation there to cease the intercept … and we have arrangements in place within the organisation, firstly to ensure that happens, secondly, we are required to report that to the Attorney-General, and thirdly, it is documented and the Inspector-General has access to that documentation.[39]

Committee comments

3.65 The recovery of listening and tracking devices will most often be conducted covertly and we consider it is appropriate to allow ASIO scope for determining the most appropriate time for such an exercise. The amendments provide this flexibility.

3.66 We note that the amendments refer only to the recovery of devices – not to the period in which devices are active. Nothing in the amendments would allow either a listening device or a tracking device to be active beyond the time specified in warrant originally authorised by the Attorney-General.

3.67 As this amendment will allow a significant enhancement to ASIO's capacity to retrieve devices, it would be appropriate for the Inspector-General to monitor closely the operation of this provision.

3.68 The Inspector-General of Intelligence and Security should report annually to the Attorney-General and the Leader of the

---

38 Attorney-General's Department, *Submission No. 9*, p. 5

39 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 14

Opposition on the frequency with which ASIO recovers listening and tracking devices outside normal warrant periods.

Item 24, section 27AA – Inspection of delivery service articles

3.69 Section 27AA will enable the Minister to issue a warrant permitting ASIO to access an article that is being delivered by a delivery service provider. The addition of this section will enable ASIO to inspect and copy articles delivered by private delivery agents in the same way as it can access postal articles.

Concern raised in evidence

3.70 The Australian Privacy Charter Council drew attention to the fact that the proposed section 27AA does not contain a prohibition on the collection of information about 'Australian citizens or permanent residents' – a prohibition which is present in a complementary section in the ASIO Act (that is, section 27A(9)).[40]

Committee comment

3.71 Warrants issued under section 27A relate to the performance by ASIO of its foreign intelligence gathering functions. A provision prohibiting the 'collection of information concerning an Australian citizen or permanent resident' is relevant in this context.

3.72 A similar provision relating to access to delivery service articles in pursuit of ASIO's domestic security and intelligence functions is not appropriate.

Item 34, paragraph 29(1)(a) - Emergency warrants

3.73 The proposed paragraph 29(1)(a) will give the Director-General greater authority to issue warrants in an emergency.

3.74 The Director-General is currently permitted to issue emergency listen device and telecommunications interception warrants, if various

40 The Australian Privacy Charter Council, *Submission No. 11*, p. 5

statutory requirements are satisfied. This amendment will allow the Director-General to issue emergency warrant for searches, computer access, tracking devices relating to persons and objects, and inspection of postal articles and delivery service articles.

Concerns raised in evidence

3.75 Joan Coxsedge expresses alarm at a provision which 'allows the Director-General to broaden the range of warrants in an emergency and tell his minister after the event'.[41] In its submission, Electronic Frontiers Australia argues that 'there should be no power for the Director-General to issue emergency warrants'.[42]

Government responses

3.76 The submission from the Attorney-General's Department notes that emergency warrants are issued only in rare circumstances: specifically, in situations where 'security will be, or is likely to be, seriously prejudiced if the action authorised by the warrant is not commenced before a warrant can be issued by the Attorney-General.' Moreover, the Director-General must immediately provide a copy of the warrant, and a statement of reasons, to the Attorney-General. An emergency warrant can only remain in force for 48 hours and can be revoked by the Attorney-General. [43]

3.77 In his evidence to our hearing the Director-General stated that emergency warrants have been issued on three occasions since 1980: once in 1981, once in 1986 and once in 1993.

> In each case … [the reason] has been a combination of the short-term unavailability of the Attorney-General and the assessed need for the warrant to come into force urgently and unexpectedly – within a matter of hours.[44]

41 Joan Coxsedge, *Submission No. 3*, p. 3

42 Electronic Frontiers Australia, *Submission No. 10*, p. 3

43 Attorney-General's Department, *Submission No. 9*, p. 7

44 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 19

Committee comments

3.78 We consider that the amendments in the Bill represent a reasonable extension of the current emergency warrant provisions. There are no compelling reasons why the Director-General should be allowed to issue emergency warrant provisions for listening devices and telecommunications interception (as at present), but not in relation to other intelligence gathering strategies.

3.79 We are reassured to note that the emergency warrant provisions have been used only sparingly in the past and that the Director-General is accountable to the Attorney-General and the Inspector-General for these decisions.

3.80 It is impractical to propose an alternative emergency warrant process involving authorisation by a panel of ministers (including the Attorney-General). By definition, emergency warrants are only used when the Attorney-General is not available to consider a warrant application.

Item 41, subsection 40(1) – Olympic Games security assessments

3.81 The proposed subsection 40(1) will allow ASIO to send security assessments directly to a relevant State authority in connection with the Year 2000 Olympics and Paralympics. At present, while ASIO is permitted to provide security assessments to State authorities, they must be transmitted through an intermediary Commonwealth agency.

3.82 The amendment will simplify the administrative procedures involved in such an exchange in the expectation that the State authorities responsible for Olympic security are likely to request a large number of such assessments.

3.83 The amendments have a sunset clause and the procedures for the provision of security assessments to State authorities will return to normal after the Year 2000 Olympics.

Concern expressed in evidence

3.84 Privacy New South Wales expressed a general concern about the effectiveness of the accountability measures surrounding the exchange of information between ASIO and state law enforcement agencies, which

were described as being based on memoranda of understanding. Chris Puplick, on behalf of Privacy New South Wales, argued that the terms of these memoranda should be subject to public scrutiny.[45]

Government response

3.85 The Attorney-General's Department explained ASIO's role in providing security assessments in relation to the Year 2000 Olympics in the following terms:

> … security vetting decisions for the Year 2000 Olympic Games will be made by the responsible State authorities. ASIO is permitted to provide security assessments to assist those decisions where a decision by a State authority would affect security connect with matters with in the functions of a Commonwealth agency.[46]

3.86 In his evidence at our hearing the Director-General said that he was expecting New South Wales authorities to request between 40 000 and 80 000 security clearances in the three month period leading up to and including the Games.[47] The majority of these requests will concern the accreditation of people to work in different parts of the Games organisation.[48]

3.87 The Director-General explained that the vast majority of the assessments will involve a simple check of whether a person has a security record: not a full scale individual background check.[49]

> Where there is a need to go beyond a basic security assessment, that will be done; where we need to check with our overseas liaison partners, that will also be done.[50]

3.88 The Attorney-General's Department also advised us that the amendments maintain the rights of a person affected by a prejudicial

---

45 Privacy New South Wales, *Submission No. 5*, p. 3

46 Attorney-General's Department, *Submission No. 9*, p. 7

47 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 20

48 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 21

49 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 21

50 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 50

assessment to be given a copy of the assessment and to be advised of their review rights.[51]

Committee comments

3.89 We recognise the scale of the security assessment task to be undertaken by ASIO in the lead up to and during the Year 2000 Olympic Games. The new administrative processes allowed by subsection 40(1) will make an enormous task more manageable.

3.90 It is expected that in the overwhelming majority of cases ASIO will be providing advice simply on whether someone has a security record. In those instances where a more detailed assessment is undertaken, and an adverse assessment is provided, we note that the usual advisory and appeals processes described in section 38(1) of the ASIO Act will apply.

3.91 We note also that the amendment has a sunset clause of 31 December 2000. It is appropriate that the arrangements for the provision of assessments and advice by ASIO and State authorities return to normal after the Year 2000 Olympic Games.

3.92 General concerns in submissions about the procedures and practices surrounding the exchange of information between ASIO and State law enforcement agencies are beyond the scope of our current task.

51 Attorney-General's Department, *Submission No. 9*, p. 8

CHAPTER 4

SCHEDULE 2 - PENALTY PROVISIONS AND SCHEDULE 3 - THE SPELLING OF 'ORGANIZATION'

Schedule 2 - Penalty provisions

4.1 At present, most of the penalty provisions in the ASIO Act describe a period of imprisonment and a fine of particular monetary value (for example, the penalty for an offence under section 18(2) is '$5000 or imprisonment for 2 years or both').

4.2 The items in schedule 2 will modify the penalty provisions within the ASIO Act by removing reference to fines of a particular monetary value, and allowing a court to impose a fine calculated in accordance with the provisions of the *Crimes Act 1914.* These provisions will allow fines to be calculated in a consistent fashion across Commonwealth legislation and in a way that reflects the value of money over time.

Schedule 3 - The spelling of 'Organization'

4.3 The items in schedule 3 will amend the ASIO Act and other legislation to amend the spelling of the word 'Organization' to 'Organisation', to reflect common practice.

Committee comments

4.4 The Committee supports the proposed amendments in schedules 2 and 3.

CHAPTER 5

SCHEDULE 4 - FINANCIAL TRANSACTION REPORTS ACT 1988

Background

5.1 Schedule 4 proposes to amend the *Financial Transaction Reports Act 1988* (the FTR Act) to allow ASIO access to financial transaction reports (FTR) information maintained by the Australian Transaction Reports and Analysis Centre (AUSTRAC).

General concerns about ASIO's access to FTR information

Concerns raised in evidence

5.2 Some submissions object to ASIO having access to FTR information.

5.3 The Financial Services Consumer Policy Centre argues that allowing ASIO access to FTR information will distort AUSTRAC's focus on combating money laundering and tax evasion.[1]

> It must be remembered that the activities of AUSTRAC are privacy intrusive and are tolerated because the public agrees that money laundering and tax evasion are serious problems, and because the public are assured that that the information is collected and used in an appropriate way for the elimination of money laundering and tax evasion. The public should not be expected to tolerate any use of AUSTRAC information outside those parameters.[2]

5.4 The Australian Privacy Charter Council expressed similar concerns, arguing that the increase in the number and type of agencies being allowed access to FTR information is subverting the assurances originally given to the community that FTR information would only be used to combat 'organised and major crime'.[3]

---

1 Financial Services Consumer Policy Centre, *Submission No. 12*, p. 8

2 Financial Services Consumer Policy Centre, *Submission No. 12*, p. 9

3 Australian Privacy Charter Council, *Submission No. 11*, pp. 5-6

Government responses

5.5 In his second reading speech, the Attorney-General argued that the amendment will allow ASIO to follow money trails associated with activities that are intended to harm Australia's national security.

> … activities that are prejudicial to Australia's national security are likely to be connected with concealed movements of money, including movements of money into Australia. It is entirely appropriate that ASIO should be able to access such potentially important information which is already available for law enforcement.[4]

5.6 The submission from the Attorney-General's Department added that the amendment goes some way to implementing international measures to fight terrorism. In July 1996, the G7 group of nations invited all nations to take measures to counteract terrorism, including measures to monitor cash transfers and bank disclosures.[5] This resolution complements work being done under the auspices of the United Nations to develop an international convention for the suppression of the financing of terrorism.[6]

5.7 At the hearing, the Director-General of Security stated that access to FTR information can be critical to ASIO's work 'especially in the area of counter espionage and also in the areas of politically motivated violence and terrorism'.[7] The Director-General also noted that the security and intelligence agencies in 'most other comparable countries in the world have… [access to FTR-type information]'.[8]

5.8 An example of the importance of FTR information to ASIO was provided in AUSTRAC's submission:

> AUSTRAC has been advised that in a number of well-known terrorism incidents, substantial funds were sent to banks in the

---

4 Hon Daryl Williams AM QC MP (Attorney-General), *House of Representatives Hansard*, 25 March 1999 p. 4364

5 Attorney-General's Department, *Submission No. 9*, p. 8

6 The Director-General of Security advised us that this convention was likely to be finalised by the end of the year (see Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 3)

7 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 3

8 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 55. Mr Richardson also remarked that 'I believe it is something of note that we do not have it [that is, access to FTR information] rather than that we are seeking it.'

> victim country to pay for the material etc used in subsequent acts of terrorism. AUSTRAC understands that FTR information could be used by ASIO as an intelligence source in relation to assessments where there are already some suspicions about a particular person in relation to a matter of national security.[9]

5.9 Elizabeth Montano, the Director of AUSTRAC, acknowledged that while it was commonly understood that AUSTRAC's function was to combat money laundering and tax evasion, the FTR Act empowers to AUSTRAC to facilitate the administration and enforcement of Commonwealth laws.[10] She noted that financial intelligence is used in combating a wide range of crimes:

> If you look at AUSTRAC's annual reports of the last few years, [FTR] information has been of enormous help in a range of matters: exotic native bird smuggling, where the financial trails of the catchers and the sellers have lead to the offenders being apprehended; finding recalcitrant, non-paying parents through the Child Support Agency.[11]

5.10 AUSTRAC's written submission also made the point that a wide range of investigatory and law enforcement agencies already have access to FTR information, including:

- all state and territory police forces;
- NSW Crime Commission;
- NSW Independent Commission Against Corruption;
- NSW Police Integrity Commission;
- QLD Criminal Justice Commission;
- Australian Bureau of Criminal Intelligence;
- Australian Federal Police;
- National Crime Authority;
- Australian Securities and Investments Commission;

---

9 Australian Transaction Reports and Analysis Centre, *Submission No. 7*, p. 3

10 Elizabeth Montano (AUSTRAC), *Transcript of Evidence*, 27 April 1999, p. 55. See also subsection 4(2) of the Financial Transaction Reports Act.

11 Elizabeth Montano (AUSTRAC), *Transcript of Evidence*, 27 April 1999, p. 55

- Australian Customs Service; and
- Australian Taxation Office and all State and Territory revenue authorities.[12]

Committee comments

5.11 ASIO is empowered by law to advise the Government on matters relating to the security of the Commonwealth and its people. Security is defined in the ASIO Act as protection from espionage; sabotage; politically motivated violence; promotion of communal violence; attacks on Australia's defence system; or acts of foreign interference.[13]

5.12 These are very significant responsibilities. They are at least as significant as those performed by the agencies that currently have access to FTR information.

5.13 It is appropriate that the ASIO have access to FTR information to the extent that such information is relevant to the performance of its duties.

Item 1, subsections 27AA(1), (2) and (3) - Access to FTR information

5.14 Subsections 27AA(1), (2) and (3) allow the Director of AUSTRAC to authorise ASIO to have access to FTR information. The authorisation is to state the FTR information, or class of FTR information, to which ASIO has access. It is proposed that the Director's authorisation take the form of a memorandum of understanding between AUSTRAC and ASIO.

5.15 Some submissions have argued that the Bill is deficient because it contains no legislative restrictions on the scope of ASIO's access to FTR information, nor any protection against misuse of the information by ASIO.[14]

---

12 Australian Transaction Reports and Analysis Centre, *Submission No. 7*, p. 3

13 See sections 17 and 4 of the ASIO Act.

14 See Financial Services Consumer Policy Centre, *Submission No. 12*, p. 8 and Australian Council for Civil Liberties, *Submission No. 14*, pp. 7-8

5.16 The Financial Services Consumer Policy Centre argues that the proposal to regulate these matters by way of a memorandum of understanding between AUSTRAC and ASIO is 'completely unsatisfactory'.

> It [the memorandum of understanding] is not a document that is available to the public. It can change at any time on the whim of only one party. It can be removed at any time without notice. It is not the subject of any regulatory oversight.[15]

5.17 The Australian Council for Civil Liberties address similar concerns, arguing that the terms of ASIO access to FTR information should be prescribed in legislation.[16]

Committee comments

5.18 The proposal to allow the Director of AUSTRAC to authorise access to FTR information by way of a memorandum of understanding is not unusual. Section 27(1) of the Financial Transaction Reports Act empowers the Director to allow access to FTR information at his or her discretion. Each of the agencies listed in paragraph 5.10 have the terms and conditions of their access described in a memorandum of understanding.

5.19 Typically, memoranda of understanding contain a level of administrative and operational detail that cannot conveniently be described in legislation. It would be impractical, for example, for Parliament to legislate for the job titles of officials who are authorised to access FTR information. Information such as this, which may be subject to frequent change, is better described in a non-legislative instrument.

5.20 It is appropriate that the control and accountability regimes for ASIO's access to FTR information be described in a memorandum of understanding. Moreover, it is consistent with the authority conferred by the Parliament on the Director of AUSTRAC.

---

15 Financial Services Consumer Policy Centre, *Submission No. 12*, p. 8

16 Australian Council for Civil Liberties, *Submission No. 14*, p. 8

The control regime for ASIO's access

Concerns raised in evidence

5.21 As well as expressing concern about the use of a memorandum of understanding to describe the control and accountability regimes governing ASIO's access to FTR information, the Financial Services Consumer Policy Centre expressed concern about the type of controls that are proposed.

5.22 In particular, the Centre objected to the following clauses in the memorandum of understanding:

- clause 10, which contemplates allowing ASIO on-line access to FTR information from ASIO premises (contrary to clause 9 of the memorandum of understanding, which states that ASIO's access will only be allowed from AUSTRAC premises);[17]

- clause 23, which although principally directed at prohibiting the downloading by ASIO of bulk FTR information for datamatching purposes, can be read as allowing the downloading of FTR information onto 'ASIO internal worksheets' (which are not defined in the memorandum);[18] and

- clause 17, which allows the Director of AUSTRAC to authorise wider data search parameters than are allowed elsewhere in the memorandum.[19]

5.23 In summary, the Centre's principal concern is that the memorandum of understanding allows more than just individual searches of AUSTRAC's database with a specific intent, and, instead, sanctions the conduct of broad-scale searches and data matching (that is, it allows ASIO to conduct 'fishing expeditions').[20]

---

17 Financial Services Consumer Policy Centre, *Submission No. 12*, pp. 9-10

18 Financial Services Consumer Policy Centre, *Submission No. 12*, p. 12

19 Financial Services Consumer Policy Centre, *Submission No. 12*, p. 12

20 Financial Services Consumer Policy Centre, *Submission No. 12*, p. 12

Government responses

5.24 Elizabeth Montano addressed these concerns by stating that the memorandum of understanding:

- ensures that authorised ASIO officers will only be able to access AUSTRAC data by 'looking for a particular person, a particular bank account number, a particular passport number – so they are furthering their existing information, not looking for new information that they would not otherwise have';[21]

- ensures that authorised ASIO officers will not be able to use 'any of our macro tools, where we look for whole classes of data in particular kinds of transactions – particular source countries, those sorts of things';[22]

- allows the search parameters to be altered beyond an individual name or bank account record, but only on a written request from the Director-General and only if the Director of AUSTRAC is provided with sufficient information to be assured that the request is in pursuit of a particular investigation and is not a 'fishing expedition';[23] and

- requires that, if any wider searches are authorised by the Director of AUSTRAC, the circumstances of the search must be referred to the Inspector-General of Security and Intelligence for his scrutiny.[24]

5.25 Ms Montano advised us that, taken as a whole, the memorandum of understanding will operate to ensure that ASIO cannot gain bulk access to FTR information held by AUSTRAC.[25]

5.26 The Director-General of Security was keen to stress that the Bill allows ASIO no more access to FTR information than is allowed to law enforcement agencies and, in fact, the memorandum of understanding

---

21 Elizabeth Montano (AUSTRAC), *Transcript of Evidence*, 27 April 1999, p. 25

22 Elizabeth Montano (AUSTRAC), *Transcript of Evidence*, 27 April 1999, p. 25

23 Elizabeth Montano (AUSTRAC), *Transcript of Evidence*, 27 April 1999, pp. 51-2. Ms Montano gives a specific example of the circumstances that might result in a wider search being sanctioned at pp. 51-2 of the transcript of evidence.

24 Elizabeth Montano (AUSTRAC), *Transcript of Evidence*, 27 April 1999, p. 24 and p. 52

25 Elizabeth Montano (AUSTRAC), *Transcript of Evidence*, 27 April 1999, p. 54

restricts ASIO's access to less than that available to law enforcement agencies.[26]

5.27 The Director-General also indicated that he expected ASIO to be a 'low volume user [of AUSTRAC's database] compared to other agencies.'[27]

Committee comments

5.28 The issue in question here is whether the memorandum of understanding strikes an appropriate balance between:

- on the one hand, the community interest in ensuring that ASIO has access to information which will help it protect the Commonwealth and its people; and

- on the other hand, the right of individuals to ensure that the privacy of their personal financial affairs is respected and that such information is not misused.

5.29 This is no easy task and we recognise the sensitivities involved.

5.30 We believe it is appropriate that, in the first instance, the memorandum of understanding should take a careful and cautious approach to finding this balance. By proposing to allow ASIO access on tighter terms and conditions than are applied to other users of AUSTRAC's database, a cautious approach has been taken.

5.31 We also accept that it is necessary to allow a degree of flexibility in such agreements, in recognition of the fact that it is not possible to foresee all of the various operational circumstances and needs that may arise.

5.32 The adoption of an initially cautious approach will allow the Inspector-General of Security, the Attorney-General and the wider-community to monitor the frequency and nature of ASIO's access. While

---

26 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 3. For example, it was noted in evidence that the Queensland Criminal Justice Commission has direct online access to AUSTRAC's database from its own premises, whereas the memorandum of understanding will only allow authorised ASIO officers to access the database from AUSTRAC premises. (See Dennis Richardson, *Transcript of Evidence*, 27 April 1999, pp. 30-31)

27 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 30

it may be appropriate at some point in the future to review the terms and conditions of ASIO's access to FTR information, it is equally important that any changes to the access arrangements be made openly and that the reasons for the change be explained and justified. Accordingly, we make the following recommendation.

5.33 Any memorandum of understanding negotiated between the Director of AUSTRAC and the Director-General of Security on access to and use of financial transaction reports information, and any revisions or modifications to such memoranda, should be presented to the Parliamentary Joint Committee on ASIO for consideration before coming into effect.

5.34 In recognition of the importance of ensuring sound monitoring and accountability measures are in place to supervise ASIO's access to FTR information we make the following recommendation.

5.35 Any memorandum of understanding negotiated between the Director of AUSTRAC and the Inspector-General of Intelligence and Security, and any revisions or modifications to such memoranda, should be referred to the Parliamentary Joint Committee on ASIO for consideration before coming into effect.

CHAPTER 6

SCHEDULE 5 - INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY ACT 1986

Background

6.1 Schedule 5 contains various amendments to the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) to strengthen the Inspector-General's ability to oversee the operations of ASIO and to monitor ASIO's proposed access to FTR and tax information.

6.2 The main amendments are to:

- make more explicit the Inspector-General's role in monitoring ASIO (schedule 5, item 1);
- ensure that tax information is not contained in the reports supplied to the relevant ministers (schedule 5, items 2 and 3);
- allow the Inspector-General to make reports under his new monitoring powers and reduce the number of steps required to obtain clearances before completing an inquiry (schedule 5, items 4, 5 and 6); and
- amend the IGIS Act secrecy provisions to permit the disclosure of information if the safety of a person may be at risk (schedule 5, items 7 and 8).

6.3 The impetus for these changes arose from the 1995 Commission of Inquiry into the Australian Secret Intelligence Service (ASIS), which recommended that the Inspector-General should focus more strongly on monitoring and oversight, rather than complaint investigation.[1]

---

1 Samuels G and Codd M, Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service, Public Edition,* March 1995, pp. 93-105

General concerns about monitoring and oversight of ASIO

Concerns raised in evidence

6.4 Concerns were raised in a number of submissions about the effectiveness of the accountability framework surrounding ASIO's operations, especially as the Bill proposes to enhance ASIO's information gathering powers.

6.5 The Australian Civil Liberties Council is particularly sceptical of the ASIO's accountability obligations and claim that '… ASIO remains a hugely secret and unaccountable agency (even acknowledging the limited role of the Inspector-General).'[2]

6.6 Electronic Frontiers Australia (EFA) expressed concern that 'Parliament may have been asked to take 'on trust' that ASIO and its Director-General will not abuse these new sweeping powers'. EFA went on to argue that:

> Only an extra-agency review of these powers can provide safeguards against the possibility of ASIO abusing these powers for the Government of the day, for the agency or an agent's personal purposes.[3]

6.7 The Australian Privacy Charter Council presented a similar point of view, arguing that 'there should be no diminution, and if possible, an increase in the level of accountability, scrutiny and safeguards applying to ASIO.' The Privacy Charter Council expressed particular concern about the level of public reporting of ASIO's activities and suggested that, as the Bill proposes to allow access to new surveillance techniques and information, it is timely to consider the reporting requirements to which ASIO is subject. In particular, the Council proposed that:

> ASIO should be required to report annually on the number and type of warrants applied for and the number of approvals or refusals … [In addition, if ASIO is allowed access to FTR and tax information]

---

2 Australian Civil Liberties Council, *Submission No. 14*, p. 4. In support of this claim, the Council draws distinction between 'the significant degree of obvious and transparent external accountability' to which law enforcement agencies are subjected when seeking to obtain a warrant from a judicial authority, compared to ASIO's process of obtaining a warrant from the Attorney-General. Privacy New South Wales also expressed little confidence in the system of ministerial authorisation of warrants as an accountability measure, arguing that 'the expansion of circumstances in which warrants can be issued calls for a more arms length process using judicial officers.' See Privacy New South Wales, *Submission No. 5*, p. 2.

3 Electronic Frontiers Australia, *Submission No. 10*, p. 4

> ASIO and the Inspector-General, as well as AUSTRAC and the Tax Commissioner, should be required to report publicly on the volume of requests for information from those two sources.[4]

6.8 Privacy New South Wales supported the proposition that public trust in ASIO's ability to exercise its powers responsibly would be enhanced by more comprehensive and candid reporting. Chris Puplick, on behalf of Privacy New South Wales, submitted that:

> There can surely be little objection to aggregated reporting on the extent to which recognised legal powers [such as the issuing of ministerial warrants] are used … [5]

Government responses

6.9 The Inspector-General of Intelligence and Security defended the scope and integrity of the arrangement currently in place to monitor ASIO's performance. In his submission he stated that:

> …any suggestion that these changes [to ASIO's intelligence gathering powers] may somehow serve as a 'Trojan Horse' for the unjustified extension of ASIO's functions, ignores the safeguards which are in place and proposed, which ensure that ASIO's activities are undertaken in an accountable and verifiable framework.[6]

6.10 Moreover, the Inspector-General argues that many of the amendments in the Bill are specifically designed to reinforce his monitoring role and strengthen ASIO's accountability framework. In particular, the Inspector-General pointed to the amendments which will require monitoring of, and reporting to the Attorney-General on:

- ASIO's compliance with the FTR Act;
- the memorandum of understanding between the Director-General of Security and the Director of AUSTRAC; and
- the ministerial guidelines which cover ASIO's handling of personal information.[7]

---

4 Australian Privacy Charter Council, *Submission No. 11*, p. 6

5 Privacy New South Wales, *Submission No. 5*, p. 2

6 Inspector-General of Intelligence and Security, *Submission No. 1*, p. 2

7 Inspector-General of Intelligence and Security, *Submission No. 1*, p. 2. See also the Acting Inspector-General's comment at our hearing about the 'quite explicit provision which

6.11 The submission we received from AUSTRAC describes in some detail the oversight arrangements to be undertaken by the Inspector-General in relation to ASIO's access to FTR information. The essential elements of the oversight arrangements (which are described in a memorandum of understanding between the Inspector-General and the Director of AUSTRAC) are that:

- the Inspector-General will routinely review 'online usage statistical reports in relation to ASIO's access to FTR information';
- the Director will notify the Inspector-General of any requests from the Director-General of Security for access to information or wider provisions than those usually used; and
- continued access by ASIO to FTR information will be dependent upon a 'clean bill of health' from the Inspector-General each year.[8]

6.12 The Commissioner of Taxation also refers to the monitoring role to be played by the Inspector-General in relation to ASIO requests for tax information.[9] An additional element to the accountability framework is the proposed amendment to subsection 3B(1AA) of the *Taxation Administration Act 1953*, which requires the Commissioner to include, in his annual reports, statements of the number of requests for tax information received from the Director-General and the number of disclosures made.

6.13 In its submission the Attorney-General's Department suggested that the amendments will allow the Inspector-General to monitor ASIO's performance more directly and frequently than has occurred before. The Inspector-General will be specifically empowered to inspect ASIO on a regular basis to 'confirm that ASIO is complying with Australian laws and with ministerial directives (and guidelines) as well as the appropriateness and effectiveness of its internal procedures'.[10]

---

acknowledges the appropriateness of the Inspector-General having a free-hand in conducting day to day monitoring.' (Ron McLeod (Office of the Inspector-General of Intelligence and Security), *Transcript of Evidence*, 27 April 1999, p. 24).

8 AUSTRAC, *Submission No. 7*, pp. 11-13

9 Commissioner of Taxation, *Submission No. 8*, p. 4

10 Attorney-General's Department, *Submission No. 9*, p. 12

Committee comments

6.14 It is no easy task to develop and maintain an appropriate accountability framework for an intelligence and security agency. It cannot be treated as an ordinary government agency and exposed to the normal processes of parliamentary scrutiny and public reporting. Neither can its operations be cloaked in total secrecy.

6.15 It is important that a balance be achieved and that mechanisms be established to give the community confidence that ASIO is performing its functions in a way that is lawful and respects individual rights and liberties.

6.16 This Bill contains a number of enhancements to ASIO's accountability regime:

- the Inspector-General will, for the first time, be empowered to conduct regular inspections of ASIO's premises;
- the Inspector-General will have the ability to review ASIO's access to FTR and tax information; and
- the Director of AUSTRAC and the Commissioner of Taxation will be able to raise any issues of concern directly with the Inspector-General.

6.17 We note that the Bill results in a shift of the Inspector-General's focus, from investigating complaints to monitoring performance, in a manner consistent with the recommendations made by the 1995 Commission of Inquiry into the Australian Secret Intelligence Service.

6.18 Improved public reporting of ASIO's activities is one important way of ensuring community confidence in ASIO. In this regard the amendment to subsection 3B(1AA) of the Taxation Administration Act to ensure public reporting of ASIO's access to tax information is commendable.

6.19 A complementary amendment to the Financial Transactions Reports Act to require public reporting of ASIO's access to FTR information, at the same level of aggregation, would be desirable. Accordingly, we make the following recommendation.

6.20 The ASIO Legislation Amendment Bill 1999 should be amended to include an amendment to the *Financial Transactions Reports Act 1988* requiring the Director of AUSTRAC to include, in AUSTRAC's annual report, information on:

(a) the number of occasions on which ASIO officers interrogated the AUSTRAC database;

(b) the number of occasions on which the Director-General of Security requested access to information on parameters wider than those available through ASIO's authorised online access; and

(c) the number of occasions on which the access requests described at (b) above were granted.

6.21 We also recognise that some of the other suggestions made to us about public reporting of ASIO's activities have merit. These issues are beyond the scope of our current task, which is to review the terms of the ASIO Bill, but we urge the Attorney-General to consider whether there is scope for more comprehensive and candid reporting from ASIO. The matter could perhaps be considered further by way of reference to this Committee.

Items 7 and 8 Subsections 34(1) and 34(1A)

6.22 Items 7 and 8 amend the secrecy provisions in the IGIS Act to allow the Inspector-General to seek professional guidance or to refer information to a police force where he believes that the well-being or safety of a person is at risk.

Reason for the provision

6.23 The Inspector-General explained the rationale for these amendments in the following terms:

> The IGIS Act makes it a criminal offence for the IGIS, or his staff, otherwise than in the course of their duties under the Act, to divulge to any person, any information obtained in the course of their duties.
>
> The IGIS sometimes receives complaints from unstable or disturbed people. Some have shown a tendency towards inflicting violence on themselves and/or others.

> In such cases, it can be important for the IGIS to be able to seek expert professional guidance, or to refer the matter to the police.[11]

Committee comments

6.24 It is appropriate that the Inspector-General be allowed to pass information to another person (perhaps a law enforcement agency) if there are reasonable grounds to believe that the safety of a person may be at risk. It is appropriate also that the legislation provide some protection to the Inspector-General for passing on information to relevant authorities in such situations.

11 Inspector-General of Intelligence and Security, *Submission No. 1*, p. 5

CHAPTER 7

SCHEDULE 6 - TAXATION ADMINISTRATION ACT 1953

Background

7.1 Schedule 6 proposes to amend the *Taxation Administration Act 1953* (the TA Act) to allow the Commissioner for Taxation to disclose tax information to an ASIO officer provided the Commissioner is satisfied that the information is relevant to the performance of ASIO's functions under subsection 17(1) of the ASIO Act.

General concern about ASIO's access to tax information

Concern raised in evidence

7.2 The Financial Services Consumer Policy Centre objects to ASIO having access to personal tax information, arguing that tax records are 'irrelevant to the purposes of ASIO' and that taxation secrecy provisions are 'an incredibly important part of the overall privacy framework for Australia'.[1]

Government responses

7.3 In his second reading speech the Attorney-General argued that the amendment will strengthen ASIO's ability to investigate those activities that involve concealed financial transactions. He cited counter espionage investigations as an example of the type of investigation that would be assisted by access to tax information. He also submitted that:

> ASIO's use of tax information will be controlled by the strict secrecy provisions of the Taxation Administration Act and will be monitored by the Inspector-General of Intelligence and Security.[2]

---

1 Financial Services Consumer Policy Centre, *Submission No. 12*. p. 16 and Chris Connolly (Financial Services Consumer Policy Centre), *Transcript of Evidence*, 27 April 1999, p. 44

2 Hon Daryl Williams AM QC MP (Attorney-General), *House of Representatives Hansard*, 25 March 1999, p. 4364. See also evidence from the Inspector-General of Intelligence that he 'envisages that the IGIS would monitor ASIO's handling of any taxation information it

7.4 The Commissioner for Taxation further clarified the control provisions further by explaining that:

> The requesting agency [in this case ASIO] becomes subject to the taxation secrecy obligations stated in the Taxation Administration Act under which the information was provided. Broadly, these preclude employees and others within the requesting agency from making a record of, divulging or communicating to any person any such tax information, except in certain prescribed circumstances.[3]

7.5 The submission from the Attorney-General's Department noted that in addition to TA Act secrecy provisions and monitoring by the Inspector-General, the 'accountability mechanisms include an annual report to Parliament on the number of ASIO requests and ATO disclosures.'[4]

7.6 At the hearing, the Director-General of Security stated that access to tax information can be critical to ASIO's work 'especially in the area of counter espionage and also in the areas of politically motivated violence and terrorism.'[5] The Director-General also noted that the proposed amendments provide ASIO with no more access to tax information than is currently available to a wide range of law enforcement agencies.[6]

---

obtained, in exactly the same manner as other ASIO activities are currently subjected to inspection. (Inspector-General of Intelligence and Security, *Submission No. 1*, p.7)

3 Australian Taxation Office, *Submission No. 8*, p. 1

4 Attorney-General's Department, *Submission No. 9*, p. 11

5 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 3

Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 3. Witnesses from the Australian Taxation Office expanded on this point by explaining that the following agencies currently have access to tax information under the same arrangements as are proposed for ASIO:

'the Australian Federal Police, a state or territory police force, the Director of Public Prosecutions, the National Crime Authority, the Australian Securities Commission, the Bureau of Criminal Intelligence, the Independent Commission Against Corruption, the New South Wales Crime Commission, the National Companies and Securities Commission, the Queensland Criminal Justice Commission (Queensland) and the Corporate Affairs Commissions established under a law of a state or territory … there is also a Bill before the House now that seeks to add the NSW Police Integrity Commission and the Queensland Crime Commission'. See Rory Mulligan and Margaret Haly (Australian Taxation Office), *Transcript of Evidence*, 27 April 1999, p. 35.

See also the Corporate Tax Association's opinion that 'Having regard to the other law enforcement agencies that already have access to taxation information, and provided the proposed safeguards are strictly adhered to, we would have no objection [to the proposed amendments]. (Corporate Tax Association, *Submission No. 6*, p. 1)

Committee comments

7.7 As we concluded above (in relation to ASIO's access to FTR information), we believe that ASIO has been charged with a significant set of responsibilities – responsibilities that are at least as significant as those performed by the agencies that currently have access to tax information.

7.8 It is appropriate that ASIO has access to tax information to the extent that such information is relevant to the performance of its duties.

7.9 We also note that the proposed amendments will impose the TA Act secrecy regime on ASIO officers when dealing with information disclosed by the Commissioner of Taxation.

Item 10, subsection 3EA(1)

7.10 The proposed subsection 3EA(1) is the key operative provision in this schedule. It allows the Commissioner of Taxation to disclose tax information to an ASIO officer provided the Commissioner is satisfied that the information is relevant to the performance of ASIO's statutory functions.

Concerns raised in evidence

7.11 The Taxation Institute of Australia (TIA) has, in essence, two main concerns about this provision:

- first, that it is inappropriate for the Commissioner to form a view about whether an officer from another organisation (ASIO) is performing functions under an Act (the ASIO Act) for which he, the Commissioner, is not responsible; and

- second, the confidentiality of tax information is at risk because (given the breadth of ASIO's functions as described in section 17(1) of the ASIO Act) it is difficult to envisage circumstances in which the Commissioner will be able to arrive at a decision to withhold information requested by an ASIO officer.[7]

7 Taxation Institute of Australia, *Submission No. 4*, pp. 2-3

7.12 The TIA proposes that the Commissioner's authority to release tax information to ASIO should be restricted to circumstances where 'ASIO is investigating a particular suspected or anticipated serious crime or security breach for which access to tax information is relevant and necessary.'[8] Such an amendment would result in ASIO having access on similar terms to that allowed to the National Crime Authority and the Australian Federal Police.[9]

Government responses

7.13 The Commissioner of Taxation explains, in his written submission, that he is currently negotiating a memorandum of understanding with the Director-General of Security to establish a framework for the operation of this provision. It is intended that this matter also be discussed with the Inspector-General of Security.[10]

7.14 The proposed operational framework was described in the following terms:

> In order to satisfy the Commissioner that the tax information [requested by ASIO] is relevant [to the performance of Asia's functions] ... , the ATO is proposing to rely on the letter containing the request to be signed personally by either the Director-General of Security, or an ASIO officer at Senior Executive Service level who has been authorised by the Director-General to make these requests, stating that:
>
> . the request is relevant to the performance of ASIO's functions;
>
> . the general nature of the matter being investigated; and
>
> . how the information will be used. …
>
> This approach will allow the Commissioner to form an opinion that the tax information is relevant for the purpose specified in the new subsection 3EA(1).[11]

7.15 The Director-General confirmed these arrangements, advising us that '… no one will be approaching the tax office below SES level and, in

---

8 Taxation Institute of Australia, *Submission No. 4*, pp. 3-4

9 Taxation Institute of Australia, *Submission No. 4*, p. 2

10 Australian Taxation Office, *Submission No. 8*, p. 3

11 Australian Taxation Office, *Submission No. 8*, p. 4

each case, I will be personally authorising [the request for tax information].[12]

Committee comments

7.16 We consider that the test proposed in subsection 3EA(1) is appropriate. In particular, we consider it is appropriate that:

- the Commissioner only disclose tax information if he is satisfied that the information is relevant to the performance of ASIO's functions;
- the Commissioner look to obtain an authorisation to this effect from the Director-General; and
- the test for disclosure refer to the statutory responsibilities that Parliament has imposed on ASIO, not to any other standards.

7.17 We do not believe it would be appropriate to restrict ASIO's access to particular 'suspected or anticipated serious crime or security breach', in the manner of the access regimes for law enforcement agencies. There is a clear difference in the roles performed by law enforcement agencies and ASIO. Law enforcement agencies investigate crimes after they have occurred, whereas ASIO investigates activities with a view to preventing harm from occurring. To require the same degree of specificity from an ASIO access request as from a police force request would risk undermining the effectiveness of ASIO investigations. Put simply, it is far preferable to allow ASIO access to information that may prevent a terrorist action, rather than waiting for the action to occur.

Item 10 - subsections 3EA(2), 3EA(3)(a) and 3EA(3)(b)

7.18 Subsection 3EA(2) imposes a general secrecy obligation prohibiting an ASIO officer (or former ASIO officer) from recording, divulging or disclosing any tax information received from the Commissioner of Taxation, from another ASIO officer or from an officer of the Inspector-General of Security. Subsections 3EA(3)(a) and 3EA(3)(b) contain two of the five exceptions to this prohibition on disclosure.

---

12 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 36

- Subsection 3EA(3)(a) provides that an ASIO officer may make a record of tax information obtained for the purposes of carrying out ASIO's section 17(1) functions; and

- Subsection 3EA(3)(b) provides that an ASIO officer may divulge or communicate the information to another ASIO officer for the purposes of carrying out ASIO's section 17(1) functions.

Concern raised in evidence

7.19 The TIA argues that the confidentiality of tax information is 'absolutely integral to the integrity of the taxation regime' and is 'instrumental in ensuring that taxpayers make full and true disclosure and comply with the taxation laws'. The TIA submits that the proposed amendments 'undermine this foundation of the taxation regime.'[13]

7.20 As an alternative, the TIA proposes the same formulation as it proposed in relation to subsection 3EA(1): that the secrecy provisions of the TA Act only be overridden in 'circumstances where ASIO is investigating a particular suspected or anticipated serious crime or security breach for which access to tax information is relevant and necessary'.[14]

Government response

7.21 At the hearing, witnesses from the Australian Taxation Office denied that the amendments weakened the confidentiality and privacy controls, thereby posing a potential threat to the integrity of the tax system. Margaret Haly argued that:

> … we think that our secrecy provisions have very tight controls and are provided with penalties that are quite severe. These rights of access [such are proposed for ASIO] are not given lightly. We believe that they do not pose a risk to the revenue but are a responsible approach to the administration of the taxation laws. [15]

13 Taxation Institute of Australia, *Submission No. 4*, p. 3

14 Taxation Institute of Australia, *Submission No. 4*, p. 3

15 Margaret Haly (Australian Taxation Office), *Transcript of Evidence*, 27 April 1999, p. 34

Committee comments

7.22 As noted above, we consider that the test described in subsection 3EA(2) for allowing ASIO access to tax information is appropriate. For the same reasons, we consider that the exclusions described subsections 3EA(3)(a) and (b) are appropriate.

7.23 It would make a nonsense of allowing ASIO access to tax information if ASIO officials were not permitted (in the normal course of duties) to make a record of the information or to disclose the information to other ASIO officers or officers of the Inspector-General of Security and Intelligence.

7.24 We consider that the secrecy obligations imposed on ASIO officers and officers from the Inspector-General of Intelligence and Security will ensure that tax information is only used in the performance of ASIO's section 17(1) functions and the Inspector-General's review functions. In relation to the secrecy obligations imposed on the Inspector-General, we note that item 3 in schedule 5 will even prevent the Inspector-General from including tax information in any investigation or monitoring reports provided to the relevant minister.

The nature of ASIO's access

Concerns raised in evidence

7.25 Some witnesses expressed concern about the possibility that ASIO was being allowed direct on-line access to tax information held by the Australian Taxation Office and that it would be possible for ASIO to conduct broad-scale data matching exercises.[16]

7.26 The Financial Services Consumer Policy Centre also repeated its concern about the use of a memorandum of understanding, rather than a legislative instrument, to secure the scope and basis of ASIO's access to tax information.[17]

16 Financial Services Consumer Policy Centre, *Submission No. 12*, pp. 17-18. Similar concerns were implied in Electronic Frontiers Australia, *Submission No. 10*, p 4 and Australian Council for Civil Liberties, *Submission No. 14*, pp. 6-8

17 Financial Services Consumer Policy Centre, *Submission No. 12*, p. 16

Government responses

7.27 The Commissioner of Taxation makes clear in his submission that the amendments do not allow ASIO direct access to information held by the Australian Taxation Office. The process by which information will be provided is described as follows:

> Once the Commissioner is satisfied that the tax information is being sought for the purpose specified in subsection 3EA(1), the ATO will gather the information sought from within the ATO. ASIO will not assist in this information gathering … The tax information to be provided will be restricted to information already in the possession of the ATO. The ATO will not seek to acquire information that may be relevant to the request from other external sources under any of its powers to access information.[18]

7.28 Taxation Office witnesses also denied that the amendments would allow ASIO 'bulk access' to tax information, thus enabling broad-scale data matching to take place. Rory Mulligan explained that neither the amendments, nor the draft memorandum of understanding between the Taxation Office and ASIO, contemplate bulk access or data matching.[19] He went on to advise that:

> We do not anticipate that we will be receiving significant numbers of requests. If we do, we will be getting back to them to find out what is going on, because that is definitely not our understanding of the particular provision.[20]

7.29 The Director-General of Security confirmed that he expected that ASIO would be making few requests for tax information, fewer even than the expected number of requests for FTR information.[21]

---

18 Commissioner of Taxation, *Submission No. 8*, p. 4. See also the following evidence at the hearing: '… we, the ATO, are the only people who have access to our knowledge, our information and our systems. When they want to receive information about a particular person or entity they give us a request. We, not the other agency, go away and search for that information and we will physically hand it over to them. The other agency has no right of access to our systems or information.' (Rory Mulligan (Australian Taxation Office), *Transcript of Evidence*, 27 April 1997, p. 33)

19 Rory Mulligan (Australian Taxation Office), *Transcript of Evidence*, 27 April 1997, pp. 59-60

20 Rory Mulligan (Australian Taxation Office), *Transcript of Evidence*, 27 April 1997, p. 59

21 Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1997, p. 34

Committee comments

7.30 By allowing the Commissioner of Taxation to 'disclose tax information to an authorised ASIO officer', rather than allowing ASIO to access ATO records, the legislation provides an appropriate measure of control over ASIO's access to tax information.

7.31 While we have no difficulty with the proposal to describe various procedural and administrative matters in a memorandum of understanding between ASIO and the ATO, we note that the memorandum is still being drafted. It is, therefore, not possible for us to be assured as to the appropriateness of its contents. We have no reason to doubt that the memorandum will be consistent with the control measures described in evidence, but, given the degree of sensitivity surrounding this issue, we believe that the memorandum of understanding should be exposed to the sort of consideration we have recommended for the memorandum of understanding between ASIO and AUSTRAC.

7.32 Any memorandum of understanding negotiated between the Commissioner of Taxation and the Director-General of Security on access to and use of tax information, and any revisions or modifications to such memoranda, should be presented to the Parliamentary Joint Committee on ASIO for consideration before coming into effect.

DAVID JULL MP

Presiding Member

6 May 1999

APPENDIX 1

LETTER OF REFERRAL

The Hon. David Jull, MP
Presiding Member
Parliamentary Joint Committee on the
Australian Security Intelligence Organization
Parliament House
CANBERRA ACT 2600

Dear Mr Jull

I refer to the Australian Security Intelligence Organisation Legislation Amendment Bill 1999 (the Bill) which was introduced into the House of Representatives on 25 March 1999.

Your Committee will be aware from briefings by the Director-General of Security that the amendments to the Australian Security Intelligence Organization Act 1979 (the ASIO Act), and to other legislation, proposed in the Bill are intended to overcome certain difficulties encountered by ASIO in performing its statutory functions.

Pursuant to paragraph 92C(2)(a) of the ASIO Act, I refer to your Committee for review those aspects of the activities of ASIO that are addressed in the Bill, and in particular the efficacy of the proposed amendments to deal with any problems faced by ASIO in carrying out those activities.

In referring those aspects of ASIO's activities to the Committee, I draw your attention to subsection 92C(4) which excludes certain matters from the Committee's functions. Naturally, my referral to the Committee excludes these matters.

I ask that the Committee report to me on the outcomes of its review by 8 May 1999.

Yours sincerely

DARYL WILLIAMS

APPENDIX 2

CONDUCT OF THE REVIEW

Our review of the ASIO Legislation Amendment Bill was advertised in *The Weekend Australian* on 17 April 1999. In addition, we invited a number of people and organisations to comment on the legislation. An invitation for submissions was also placed on our web site (www.aph.gov.au/house/committee/pjcasio/index.htm).

A public hearing was held in Canberra on 27 April 1999. Appendix 4 contains a list of witnesses who appeared at this hearing. The transcript of the evidence taken at the hearing can be obtained from the database maintained on the Internet by the Department of Parliamentary Reporting Staff (www.aph.au/hansard/joint/committee/ comjoint.htm) or from the Committee secretariat.

We also received 16 written submissions to our review. A list of submissions is at Appendix 5. The submissions are available through our website or from the secretariat.

APPENDIX 3

CLAUSE BY CLAUSE COMMENTS

The following table lists specific concerns raised in submissions to our review and provides a reference where those concerns have been addressed by government witnesses.

The following abbreviations have been used:

ACCL	Australian Council for Civil Liberties
AIIA	Australian Information Industry Association
APCC	Australian Privacy Charter Council
Coxsedge	Ms Joan Coxsedge
EFA	Electronic Frontiers Australia
FSCPC	Financial Services Consumer Policy Centre
Sub	Submission
TIA	Taxation Institute of Australia
Trans	Transcript of Committee hearing held 27 April 1999

Schedule and item	**Comments**	**Government response**
1 - 5	Concerns ASIO work is being privatised. Coxsedge (Sub 3: p. 2) Which organisations will have access to ASIO services? Coxsedge (Sub 3: p. 2)	Trans: pp. 5-7 Trans: p. 5
1 - 11	How to ensure that recovering a listening device will not be used to intimidate? Coxsedge (Sub 3: p. 2)	Trans: p. 12, pp. 14-15
1 - 16	How will you ensure that access to data is not used in a 'fishing expedition'? Coxsedge (Sub 3: p. 2) Who decides what will be relevant in relation to examining data? Coxsedge (Sub 3: p. 2) How will increasing time limit for search warrants 'substantially assist in the collection of intelligence'? Coxsedge (Sub 3: p. 2) ASIO should not have power to alter, delete or add data to a computer. Coxsedge (Sub 3: p. 2); EFA (Sub 10: pp. 2-3); APCC (Sub 11: p. 4); FSCPC (Sub 12: p. 7); ACCL (Sub 14: p. 6)	Sub 9: p. 3 Sub 9: p. 3 Trans: p. 11, p. 14; Sub 9: pp. 5-6 Trans: p. 12, p. 57; Sub 9: p. 3

1 - 16	Proposed changes to section 25A should be subject to further Parliamentary scrutiny. EFA (Sub 10: p. 3); FSCPC (Sub 12: p. 6); AIIA (Sub 13: pp. 1-2); ACCL (Sub 14: p. 5) The maximum duration of a warrant should remain at 7 days. EFA (Sub 10: p. 4); APCC (Sub 11: p. 4) The proposed change to section 25(2) is fundamental and deserves serious justification or amendment. APCC (Sub 11: p. 4); FSCPC (Sub 12: p. 4); ACCL (Sub 14: p. 8)	Trans: pp. 11-12; Sub 9: p. 3 Trans: p. 11, p. 14; Sub 9: pp. 5-6 Trans: pp. 44-45, p. 47, pp. 56-57
1 - 22	The power to enter premises should be restricted to the period when the warrant is in force. Coxsedge (Sub 3: p. 2); APCC (Sub 11: p. 5); EFA (Sub 10: p. 3)	Trans: p. 11, p. 14; Sub 9: pp. 5-6
1 - 23	The use of tracking devices should be limited to 7 days. EFA (Sub 10: p. 3) By definition, it will be necessary to use a tracking device to locate it so that it may be recovered. APCC (Sub 11: p. 5)	Trans: pp. 15-16 Trans: pp. 15-16
1 - 24	How to protect articles in transit from unauthorised inspections? Coxsedge (Sub 3: p. 2) The Committee should explore the absence of protection in section 27AA for Australian citizens' and permanent residents' postal articles, as contained in subsection 27A(9). APCC (Sub 11: p. 5)	See subsection 27AA(1) Subsection 27A(9) does not refer to postal articles.
1 - 29	How will ASIO keep track of extended search warrants? Coxsedge (Sub 3: p. 2)	Trans: pp. 3-4, p. 14 See subsection 8(1)(a)(iv) of the *Inspector-General of Intelligence and Security Act 1986*
1 - 33	How will ASIO manage foreign intelligence matters in light of ASIS' role? Coxsedge (Sub 3: p. 2)	Trans: p. 17
1 - 34	How will new emergency warrants be dealt with? Coxsedge (Sub 3: p. 3) There should be no power for the Director-General to issue emergency warrants and the signature of three ministers should be required to issue a warrant. EFA (Sub 10: p. 3)	Trans: pp. 19-20; Sub 9: p. 7 Sub 9: p. 7

1 - 37	Is there a sunset clause on Olympic Games activity? Coxsedge (Sub 3: p. 3)	Sub 9: p. 7; Trans: pp. 20-21
1 - 39	In which circumstances will ASIO be allowed to communicate security assessments? Coxsedge (Sub 3: p. 3)	Sub 9: pp. 7-8; Trans: pp. 20-21
4	The Committee should insist on better justification for direct access to the AUSTRAC database. APCC (Sub 11: p. 6) ASIO should not have greater access to AUSTRAC records. FSCPC (Sub 12: pp. 8-11) If ASIO is granted greater access to AUSTRAC records, data matching, bulk and other access should be governed by legislation, not an MOU. FSCPC (Sub 12: pp. 8-14); ACCL (Sub 14: p. 7)	Trans: pp. 23-24, p. 51, p. 55 Trans: pp. 23-24, p. 51, p. 55 Trans: p. 52, pp. 53-55
5	The Inspector-General should report publicly on the volume of requests for access to AUSTRAC and taxation information. APCC (Sub 11: p. 6)	Sub 9: p. 11
6	Why is ASIO seeking powers to access taxation information directly, instead of through other law enforcement bodies? Coxsedge (Sub 3: p. 3) It is inappropriate for the Commissioner of Taxation to determine whether or not an ASIO officer is performing duties under section 17(1) of the ASIO Act. TIA (Sub 4: 3) The scope of subsections 3EA(1) and 3EA(2) are too broad unless restricted to a particular suspected or serious crime or security breach. TIA (Sub 4: 3) ASIO should not have greater access to taxation records. FSCPC (Sub 12: pp. 16-8) If ASIO is granted greater access to taxation records, data matching, bulk and other access should be governed by legislation, not an MOU. FSCPC (Sub 12: pp. 16-18)	Trans: p. 59 Sub 8: p. 5 Trans: p. 59 Trans: p. 59 Trans: pp. 59-60

APPENDIX 4

WITNESSES AT PUBLIC HEARING

Tuesday, 27 April 1999

Attorney-General's Department

Norman Reaburn, Deputy Secretary

Norman Bowman, Acting Principal Legal Officer

Office of the Inspector-General of Intelligence and Security

Ron McLeod, Acting Inspector-General of Intelligence and Security

Financial Services Consumer Policy Centre

Chris Connolly, Director

Australian Security Intelligence Organization

Dennis Richardson, Director-General of Security

Australian Taxation Office

Margaret Haly, Assistant Commissioner, Law Design and Development

Rory Mulligan, Acting Assistant Commissioner, Internal Assurance

Australian Transaction Reports and Analysis Centre (AUSTRAC)

Elizabeth Montano, Director

APPENDIX 5

INDEX OF SUBMISSIONS

Submissions

1	Office of the Inspector-General of Intelligence and Security
2	The Australian Privacy Charter Council
3	Ms Joan Coxsedge
4	Taxation Institute of Australia
5	Privacy New South Wales
6	Corporate Tax Association
7	Australian Transaction Reports and Analysis Centre
8	Commissioner of Taxation
9	Attorney-General's Department
10	Electronic Frontiers Australia
11	The Australian Privacy Charter Council
12	Financial Services Consumer Policy Centre
13	Australian Information Industry Association Ltd.
14	Australian Council for Civil Liberties
15	Australian Transaction Reports and Analysis Centre
16	Attorney-General's Department