



COMMONWEALTH OF AUSTRALIA

# Official Committee Hansard

JOINT SELECT COMMITTEE ON THE INTELLIGENCE  
SERVICES

**Reference: Review of intelligence services bills**

TUESDAY, 31 JULY 2001

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

## **INTERNET**

The Proof and Official Hansard transcripts of Senate committee hearings, some House of Representatives committee hearings and some joint committee hearings are available on the Internet. Some House of Representatives committees and some joint committees make available only Official Hansard transcripts.

The Internet address is: **<http://www.aph.gov.au/hansard>**

To search the parliamentary database, go to: **<http://search.aph.gov.au>**

**JOINT SELECT COMMITTEE ON INTELLIGENCE SERVICES**

**Tuesday, 31 July 2001**

**Members:** Mr Jull (*Chair*), Mr Andrews, Mr Brereton (*Deputy Chair*), Mr Forrest, Mr Hawker, Mr McArthur, Mr McLeay, Mr Melham and Mr O’Keefe and Senators Calvert, Coonan, Faulkner, Greig, Sandy Macdonald and Ray

**Senators and members in attendance:** Mr Andrews, Mr Brereton, Mr Jull, Mr McArthur, Mr McLeay, Mr Melham and Mr O’Keefe and Senators Faulkner, Greig, Sandy Macdonald and Ray.

**Terms of reference for the inquiry:**

To inquire into, and report upon:

- (a) the Intelligence Services Bill 2001 and the Intelligence Services (Consequential Provisions) Bill 2001; and
- (b) the provision in the Cybercrime Bill 2001 relating to the Australian Secret Intelligence Service (ASIS) and the Defence Signals Directorate (DSD)—Liability for Certain Acts.

**WITNESSES**

<b>BLICK, Mr William James, Inspector-General of Intelligence and Security, Office of the Inspector-General of Intelligence and Security .....</b>	<b>41</b>
<b>MacGIBBON, Dr David John, private capacity.....</b>	<b>9</b>
<b>O’GORMAN, Mr Terence Patrick, President, Australian Council for Civil Liberties.....</b>	<b>24</b>
<b>WEEDING, Mr Mark James (Private capacity).....</b>	<b>2</b>



**Committee met at 1.42 p.m.**

**CHAIR**—I declare open this hearing of the Joint Select Committee on the Intelligence Services and welcome witnesses and members of the public. The committee has been appointed by the parliament to inquire into and report on the proposed legislative reforms in the *Intelligence Services Bill 2001*, the *Intelligence Services (Consequential Provisions) Bill 2001* and the provision in the *Cybercrime Bill 2001* relating to the Australian Secret Intelligence Service, ASIS, and the Defence Signals Directorate, DSD—liability for certain acts.

The Intelligence Services (IS) Bill reflects the findings in the 1995 commission of inquiry into the Australian Secret Intelligence Service by seeking to place ASIS on a statutory footing. For the first time, the functions of ASIS and DSD are set out in legislation. Some of the key features of the IS Bill include: the establishment of a parliamentary committee for ASIO and ASIS, which will review the administration and expenditure of ASIO and ASIS; the provision of immunities for both ASIS and DSD; and privacy provisions. The minister responsible for both ASIS and DSD must make written rules regulating the communication within government and retention of intelligence information concerning Australians and Australian corporations. The committee will examine these and other aspects of the bills and report its findings no later than 20 August 2001.

Today the committee will take evidence from Mr Mark Weeding, Dr David MacGibbon, the Australian Council for Civil Liberties and the Inspector-General of Intelligence and Security. Tomorrow the committee will continue with public hearings and take evidence from the key intelligence agencies, including DSD, ASIO and ASIS.

[1.44 p.m.]

**WEEDING, Mr Mark James (Private capacity)**

**CHAIR**—I welcome Mr Mark Weeding to today's hearing. Although the committee does not require you to give evidence under oath, I should advise you that the hearings are legal proceedings of the parliament and warrant the same respect as proceedings of the House of Representatives or the Senate. To give false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Do you wish to make some introductory remarks before we go to questions?

**Mr Weeding**—I would like to advise the committee of a little of my background and what brings me to some research in this area, and then touch on a couple of points in my submission. As some members of the committee will be aware, and as I said when I appeared here last year before the ASIO committee's inquiry, my background is in academic research into the accountability structures of Australia's intelligence agencies. I completed an honours degree a couple of years ago in that area, and I am working on a PhD in the same field. Primarily I come to you with a background in looking at the development of ASIO's accountability structures, particularly over the past 10 to 15 years, so that I can bring to bear some of the knowledge that I have gained along the way. To go to the specifics, the first point in my submission is about clause 6(1)(e), which relates to the functions of ASIS. Paragraphs (a) to (d) spell out fairly clearly in general terms what the functions of ASIS are, and then subclause (1)(e) provides that ASIS can:

undertake such other activities as the responsible Minister directs relating to the capabilities, intentions or activities of people or organisations outside Australia.

I do not have a particular difficulty with that clause. With all forms of ministerial oversight, it is necessary for the minister to have power to instruct in areas where the legislation does not provide that level of detail. My problem is that there should be stronger accountability in place when that part of the legislation is going to be used. If the bill is intended to outline the functions of ASIS, it should do so. The wording of paragraph (e)—that is, 'such other activities as the responsible Minister directs'—does not fulfil the strong sense of accountability.

I note that ASIS has always operated under ministerial directive and that the inquiry commissioners in their public report in 1995 said that legislation would never overcome the need for some form of ministerial directive to deal with the specifics of operational issues and so forth. The accountability structures that should be put in place should be stronger than is evident in the bill. There needs to be an examination of the balance of ASIS's activities and how often its activities will fall under paragraph (e) relating to ministerial directive rather than under the first four paragraphs of subclause (1).

The second point in my submission concerns liability for certain acts. I note that the explanatory memorandum argues that the clause is intended to overcome difficulties with certain current Australian laws in the agency's performance of its legitimate functions. If other Australian laws affect ASIS's and DSD's functions, perhaps there should be an examination of those laws with a view to amending them, rather than applying what appears to be carte

blanche—I say ‘appears’ because there are some qualifications in it—or broader capacity for ASIS and DSD to breach Australian law than the intent given in the explanatory memorandum.

The explanatory memorandum clearly says that the clause is to circumvent the unintended consequences of certain Australian laws. On my reading, that is not what the legislation says. The legislation potentially provides much broader scope for breaching Australian law. There may be genuine reasons for that. It may simply be the case that technology has developed more quickly than the law has been able to develop, so it is necessary for Defence Signals Directorate, for example, to make use of technologies that otherwise would be illegal in a law that might have been around for only three or four years—technology moves faster than laws do. If that is the reason behind that clause, I have no problem with it at all, but its current wording and the justification for it do not seem to sit together particularly well.

The next point I would like to make is regarding section 19, ‘Briefing the Leader of the Opposition about ASIS’. I have noted in my submission that the ASIO Act and this bill apply different forms of words to that sort of briefing. My recommendation would be that briefing of the Leader of the Opposition be enshrined in the bill as a right rather than, as it is worded at the moment, that the Director-General may, with the authorisation of the Prime Minister, brief the Leader of the Opposition about ASIS.

Samuels and Codd, the commissioners in the 1995 inquiry, make three very valid points in relation to formalising and regularising briefings of the Leader of the Opposition. The first is that an obligation to provide those sorts of briefings to senior parliamentarians is a form of parliamentary accountability. In this area, where full accountability to parliament is necessarily limited, the opportunities to provide accountability should be strengthened wherever possible. The second point is the importance of bipartisanship in issues of national security and international relations, and the third point is that the briefings provide a means by which the alternative government can maintain familiarity with the agency so that when or if they do return to power they have got some understanding at the highest level of what the agency does and what current policies it operates under.

Supporting this argument for regularising briefings of the Leader of the Opposition, the Director-General of ASIS at the time of that inquiry in 1995 considered that his responsibility for briefing the opposition leader should be more clearly defined and should be more in accord with the ASIO basis of a set schedule. I understand that briefings of the Leader of the Opposition by ASIS do go on. It has been a matter of practice for some time, but I think there is the opportunity to regularise that within the legislation.

Finally, I note in my submission that the current Parliamentary Joint Committee on ASIO is to be reconstituted to include ASIS as well. Over a number of years there have been some concerns raised, and the *Hansard* record bears this out, over the role of the ASIO committee and whether its role is too restricted. I have not formed a position as to whether the role should be expanded to look more into broad policy matters relating to that area. Again, I think it would be a small step forward in further developing the accountability of ASIS.

In concluding my opening remarks, I think that, in general terms, the legislation is a good thing. Having looked at the development of the accountability for ASIO over the past 10 to 15 years, it seems to have been done through a series of incremental steps, and this bill seems to be

the start of a similar process for both ASIS and DSD. What it does is to set up a committee which has the opportunity to look at the administration and finances of ASIS, which is something that we have not had before in that formalised structure. So that is a good step forward.

There are a number of other areas in the bill which represent incremental improvements in accountability. I would like to stress that I am, in general, in favour of the bill. I have some specific concerns about the matters that I have raised in that I do not think the opportunity to improve the accountability has been taken quite far enough.

**CHAIR**—I was going to open up on that because you gave evidence before the ASIO committee on a previous occasion. What improvements have you seen in the system since those last reforms? Do you really think that, because the ASIO committee cannot physically get into the operational areas, that has been detrimental in terms of some of the oversight that it has provided?

**Mr Weeding**—It depends on what you mean by ‘detrimental’. It is definitely a weakness in the public accountability system. It is also a very strong weakness in respect of parliamentary accountability. The committee charged with the oversight of the agency does not have the capacity to inquire into the full range of activities that the agency pursues. Reasons were given in evidence last year by ASIO as to why those limitations are there and reference is continually made to the role of the Inspector-General as the appropriate oversight mechanism.

It is hard to say whether there has been an improvement because there has been very little to examine in public forums. The ASIO web site came online just prior to last year’s inquiry. That was a significant step forward for that organisation, but since then there has been very little information in the public arena to be able to base a judgment on.

**CHAIR**—Are you aware of the ASIS web site?

**Mr Weeding**—Yes, I am. Unless it has been updated in the last week, the amount of information on that site is pretty cursory.

**CHAIR**—Ideally, how far should a committee be able to delve into operational areas? You are not suggesting that it should be open slather?

**Mr Weeding**—No. I am suggesting that it should be an incremental process rather than open slather. Given the nature of the organisations, they are going to remain conservative in their view of how much information should be in the public domain. With congressional committee oversight in the United States, they have access to a lot more information than we do here and no major difficulties have been found there with information given in confidence to a committee being leaked to the public or to the press. It would be a good accountability mechanism for the heads of these agencies to know that, every now and then, they have to front up before a body of parliamentarians who have the capacity to quiz them in more detail than they are allowed at present. There should be the recognition that they are not just answerable to their ministers and that they have to front before a body like this to answer questions. That would be a stronger mechanism than what we have at the moment. I do not know where the line should be drawn in respect of how much the committee should do, but there is potential for it to do more.

**Senator SANDY MACDONALD**—Mr Weeding, I do not find your reservations about immunity for civil and criminal liability very convincing. You say, ‘Change the domestic law, but don’t provide the limited immunity from legislation.’ Can you elaborate a little more on your concerns? Are you aware of similar immunity provisions that apply to these sorts of organisations in other countries?

**Mr Weeding**—No, I cannot say that I am aware of similar sorts of immunity. The first point that struck me about this section when I read it was that ASIS is able to commit acts inside Australia in support of overseas operations which would otherwise be illegal. The first thing that struck me about that was that part of the role of the Inspector-General is to inquire into illegal acts committed by these agencies. It occurred to me that there was a potential problem there in that this legislation potentially says to ASIS that, within certain boundaries, certain otherwise illegal activities are okay. However, those same activities would normally come under the inquiry realm of the Inspector-General.

**Senator SANDY MACDONALD**—But they are secret organisations. They are tightly controlled from Australia. If the information they were searching for was available publicly, they would not have to be covert.

**Mr Weeding**—Certainly.

**Senator SANDY MACDONALD**—Clearly, decisions are going to be made in Australia that might, in theory, breach Australian law. In theory, therefore, those people should be provided with immunity from prosecution, limited or otherwise—but surely just immunity from prosecution.

**Mr Weeding**—If that is the intention of the legislation, I suggest that that is what the legislation should say. At least the explanatory memorandum should refer to that point rather than to what it does at the moment, which is to state that it is to avoid the unintended consequences of Australian laws. I feel that the rationale that has been given is not strong enough for the legislation as it has been drafted.

**CHAIR**—A bit of a fudge do you think, Mr Weeding?

**Mr Weeding**—I would not go that far. It just seemed to gloss over what is potentially one of the most contentious areas of the legislation.

**Mr BRERETON**—Taking you to the suggestion that the rights of the Leader of the Opposition for confidential briefings should more closely follow the ASIO model than this, would you elaborate on the differences between the two models and give us some idea of how you would see that working in practice? In your view, would it be at the request of the Leader of the Opposition, or would it be done on a regular basis?

**Mr Weeding**—The [Intelligence Services Bill 2001](#) states that the Director-General may, with the authorisation of the Prime Minister, brief the Leader of the Opposition in the House of Representatives about ASIS. Part 2 of section 19 says that the Leader of the Opposition may at any time request the Prime Minister to authorise the Director-General to give such a briefing. So, within this system, the mechanism is there for the Leader of the Opposition to request a

briefing. I think there is a very slight difference between regularising it perhaps on a six-monthly basis and what is in the bill at the moment. I am not certain of the time frames of similar briefings that happen with regard to ASIO or informal briefings that already occur with regard to ASIS, but I would imagine that they would predominantly be issues based. It is good government practice to give the Leader of the Opposition a heads-up if there are issues coming in this sort of field.

I think that regularising those sorts of briefings provides a very clear indication to the organisation, and moreover to the public, that there is regular communication between the alternative government and this organisation. In terms of the limited amount of information the parliament receives on ASIS, I think it also sends a stronger message to the parliament that these organisations are under sound control.

**Senator ROBERT RAY**—Let me put a different argument to you: the more you involve the Leader of the Opposition, the more you lock him in to not being able to make criticisms because he has been briefed on a confidential basis. To some extent, some of these briefings—not necessarily in this area but in other areas—are rejected for the reason that oppositions are there in an adversarial sense to put pressure on scrutiny, and too regular a briefing reduces that. It reduces all his colleagues as well because the suspicion would be that the Leader of the Opposition has informed them to go on the attack when he has not. Isn't it a two-way street here?

**Mr Weeding**—I think it is, and I agree entirely, but it is a matter of balance between those potential dangers, if you like, and the strengthened accountability that you can have through having a regular briefing. It may be the case that the Leader of the Opposition requests a briefing on certain issues. I note in the legislation that briefing on operational issues remains only with the approval of the Prime Minister, so we would be talking about briefings regarding ASIS in a more general sense than operational details. I do take your point that in an adversarial system it can raise some potential problems. With the current system of informal briefings, as I understand, those problems would potentially still be in evidence.

**Senator ROBERT RAY**—The difficulty is that we have an adversarial system, but in two or three areas we like to demark some bipartisanship, and this happens to be one of them. It is not clear, I agree.

**Mr Weeding**—Yes.

**CHAIR**—I thought it was interesting that in your conclusion you suggested that there should be a review of this legislation, perhaps even an ongoing review every three years as to how this is developing. Would you like to elaborate on that?

**Mr Weeding**—Putting ASIS on a legislative basis is a new thing. I think it is important for the agency, for the parliament and for the public to ensure at some point that the legislation is operating as intended and that there are not unintended consequences which affect the capability of the agencies to perform their duties and so on. I have no doubt that the bill has been drafted in such a way as to try to avoid that. But in three years time, with who knows what changes in technology and international affairs, there may be issues within ASIS and DSD that need to be revisited. That is my main reason for suggesting that. Further, I do not think periodic review of

legislation is a bad thing in a more general sense. Where legislation is breaking new ground rather than tidying up older ground, I believe it can possibly bring even greater benefits.

**Senator SANDY MACDONALD**—I think you make the point that this has been an incremental development of the accountability process, first over ASIO and now over ASIS. I think you are correct in that, if that is what you say, because certainly the ASIO committee has pushed the envelope, so to speak, over the time it has been in existence. You make the point about the possibility that the committee has an oversight of operational aspects of these organisations. To what extent could that happen? What ideas have you got in that regard?

**Mr Weeding**—I believe the chairman asked me a similar question a few moments ago as to what the role of the committee is in looking at the operational nature of these organisations, and it is not something that I have a firm position on. I understand that there are inherent difficulties and possibly some fear within the agencies concerned about releasing too much information. It has been mentioned previously that the role of the ASIO committee as it stands at the moment is fairly limited. I do note that the committee that is proposed in this legislation has the capacity to effectively inquire into matters of its own motion, which is another incremental, good improvement.

Regarding operational matters, I do not think it should be the role of the committee to look at the broad policy of the government in the direction that it takes. There are the National Security Committee of Cabinet, the Secretaries Committee on Intelligence and Security and other organisations to provide that sort of policy direction. I think I would probably more be able to give you a list of what I do not think they should be able to look at operationally rather than what they should be able to look at. But, without an in-depth knowledge of the organisation, I cannot tell you what is left. I think in terms of their general policy direction, if you like, there are mechanisms in place that already do that. I do not think a joint committee would be of any value in pursuing that sort of position.

**Senator SANDY MACDONALD**—Do you think it would be a good idea if the joint committee in time oversaw the whole umbrella of the security apparatus, including ONA?

**Mr Weeding**—It appears by bringing ASIS into the present committee structure effectively that that is what it may be heading towards, although within the intelligence community I think there is always a good argument to be made for having an independent, analytical body so that the collection and the analysis have the opportunity to be kept separate.

**Senator FAULKNER**—But isn't there a slight logical inconsistency in the concept of a review after three years by the committee, given how DSD would fit into that review? You properly say, I think, in your submission that the Inspector-General and the joint parliamentary committee have a look at this, but isn't there a little bit of a weakness or inconsistency given the proposal in relation to the different ways the committee might relate to ASIS and DSD?

**Mr Weeding**—I take the point, and it may be that a review in three years should be limited to those aspects of the bill which affect ASIS. But, I take your point: if you are reviewing the legislation then why not?

**Senator FAULKNER**—You do make the point earlier in your submission too about the original proposals of Samuels and Codd in relation to the principles of accountability and control guiding ASIS equally applying to DSD. Have you given any thought, firstly, to what you consider at the moment to be the adequacy of the current parliamentary oversight of DSD? Is this adequate or is there an inadequacy in the bill that is before the parliament at the moment?

**Mr Weeding**—DSD is not an area that I have had a great deal of experience in in doing my research. Part of the reason for that is the lack of information available. There are better people. For example, Desmond Ball has far more experience within the academic field of looking at DSD. I take your point, but I am sorry I cannot answer.

**Senator FAULKNER**—I am only asking from the point of view of the principle, if you like, in terms of the parliamentary role.

**Mr Weeding**—I think in terms of the principle of parliamentary accountability, there are good grounds to ensure that the parliament and the public can be confident in what DSD are doing; but how you actually achieve that mechanism, I am not certain.

**CHAIR**—Mr Weeding, thank you very much indeed for appearing before the committee today. We will send you a transcript and the secretary will be in touch if we need any further information.

**Mr Weeding**—Thank you, Chairman.

[2.15 p.m.]

**MacGIBBON, Dr David John, private capacity**

**CHAIR**—I welcome Dr David MacGibbon, a former senator for Queensland, a former member of the joint parliamentary committee on the Australian Security Intelligence Organisation. He has had a great deal of interest over the years in these matters. Although the committee does not require you to give evidence under oath, I should advise you that the hearings are legal proceedings of the parliament and warrant the same respect as proceedings of the House or the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Would you like to make some introductory remarks before we proceed to questions?

**Dr MacGibbon**—I would like to thank the committee for inviting me to appear before it, and I am also grateful for the indulgence you have granted me in allowing me to appear without submitting a written account. Quite apart from my figure, I do not look like a trained typist and I have no secretarial services to support me.

I do have an interest in this subject, as part of my interest in national security issues over many years. In June 1986, the Australian Security Intelligence Organisation Bill was amended as a consequence of the Hope royal commission. Part 5A created the joint parliamentary committee, the first approach in our parliament to having oversight of any intelligence agency. Senator Peter Durack, a former Attorney-General, was my party's representative from the Senate on that committee. After a short while, I replaced him. Despite my eagerness and enthusiasm to get on to the ASIO committee, I tendered my resignation as it was perfectly clear, after a while, that continued service was pointless. After the election in 1996 I rejoined the committee as presiding member, relinquishing that post to become Chairman of the Joint Standing Committee on Foreign Affairs, Defence and Trade.

The powers and duties of the ASIO committee are defined with great clarity in the ASIO Act. There is nothing the committee, as a committee, can do about altering them. While presiding member, I did a great deal of research privately into contemporary overseas practices in relation to the oversight of intelligence agencies, and I put thought into what was required in our case. Coincidentally with this research, I was asked to make a report on my findings. So much for my background on this issue.

The terms of reference of your inquiry cover a vast ambit. Certainly there is far more detail there than whoever drew up the terms of reference appreciated at the time of writing. There are some very important fundamental principles involved and practical details, some of which have no clear right or wrong answer; and their resolution will call for considered judgment. This afternoon I want to confine my comments to a very narrow front—namely, the composition and role of the parliamentary joint committee, and matters that flow from that.

The central point on which my argument is based and from which everything flows is the absolute requirement of effective parliamentary accountability. I will argue that the Intelligence Services Bill will provide no improvement or advance in parliamentary oversight, let alone accountability, of the intelligence agencies than what exists at present. What exists at present is quite unacceptable.

No principle is more important in a democratic society than the accountability of its elected representatives. It is the most powerful but rarely noted concern of the populace. With higher educational levels and vastly improved gateways for information transfer as a result of technology, the demand to know is burgeoning. While the public can only express their approval or disapproval at election times, at all times they want to know where the money that is being taken from them in taxes is going and how it is accounted for—even if they strongly disapprove of where it is going.

There are wider issues than simply financial accountability. Accountability must involve making the executive government, the ministry, explain what it is doing and why. Ministries operate under unrelenting pressures in a highly adversarial environment. It is perfectly natural that they should have a great tendency to expose themselves as little as possible.

Despite this, the parliament has changed radically, in line with community expectations, with respect to accountability. Here we are discussing a bill this afternoon, which was brought in by a Liberal government, to create a new committee for intelligence oversight. Yet in 1986—and I remember it very clearly—when the ASIO Act was amended to create the first such committee, the coalition trenchantly opposed the move. Now, quite properly, they are attempting to satisfy community expectations.

In response to accountability, democratic governments go down two broad paths which are usually complementary rather than adversarial. Those paths are the development of the committee system and the creation of statutory independent offices. Great expansion in the committee system, which brought a quantum leap in accountability to the parliament, came in the Whitlam years, most importantly with the creation of the Senate estimates committees. No minister now would argue against the committee system the way Dick Casey did in the late 1940s or early 1950s, when the Joint Committee on Foreign Affairs and Defence was being formed. The pathways now are all in place and it is only the political will of the parliament to use them that limits the accountability of the executive government in all areas, except in the area of the intelligence services. Having made a statement as sweeping as that, I should in all honesty acknowledge the great difficulty in getting accountability in some sensitive political areas, as anyone who has been in opposition in the Senate will confirm.

The other pathway is by the creation of independent authorities with the requisite power to audit the actions of governments and government agencies. Such bodies as the Auditor-General, the ANAO and the Inspector-General of Intelligence and Security are well-known examples. They have an essential role to play in accountability, but by themselves they are not sufficient. In the case of the intelligence agencies, they are all we have apart from ministerial accountability. How effective are these two modalities? Ministers responsible for the intelligence agencies are all senior ministers with great administrative loads. The Prime Minister is responsible for ONA and, irrespective of party, no prime minister has time on his hands. The defence minister, with the most complex and intellectually demanding of all portfolios, cannot delve into the finer details of his two agencies, DSD and DIO. The Foreign Minister is frequently out of the country, while the Attorney-General has arguably the highest workload of all.

The Inspector-General of Intelligence and Security was established in 1986. All the appointees have discharged their duties faithfully and well. Their primary task is to ensure that

---

the agencies stay within the law and that there are no breaches of human rights, not that that has been a characteristic of our agencies in the past. They also have an important role as ombudsmen and in the grievance resolution field. However, if you look at the Inspector-General of Intelligence and Security Act, in section 4 you will find that the objects of the act are:

- (a) to assist Ministers in the oversight and review ...
- (b) to assist Ministers in ensuring that the activities of those agencies are consistent with human rights; and
- (c) to allow for review ...

While the Inspector-General does make an annual report to the parliament, without putting too fine a point on it, his responsibility is to the executive government, not to the parliament. While accountability is the dominant reason for parliamentary oversight through an effective committee system, there are other benefits that the committee brings to the table: the parliamentary committee can act as an effective safety valve. Intelligence agencies are all small, secretive, inward looking and staffed by intelligent people, often with strong personalities and individualistic tendencies. It is a fact of life that conflict of personalities is a common factor in such organisations, where it is difficult or impossible to put space between people with conflicting points of view. In these organisations it has a major effect on morale and, therefore, operational effectiveness suffers. In the worst case it sometimes blows out and erupts into the public arena.

The Inspector-General has a vital role to play in this dimension, but he is often seen as part of the administration and therefore part of the problem. In these cases a committee can offer itself as an impartial and objective arbiter. The other benefit of a committee is that it is a two-way channel of communication between the agency and the parliament. The committee provides a vehicle for the education of the parliament on the broad needs and objectives of the agencies. Conversely, there is often untapped in the parliament experience in life and public affairs in general which could usefully be brought to bear for the advantage of the agency.

One of the most succinct statements I have read in defence of oversight by a committee is to be found in the House of Lords *Hansard* of 13 January 1994 when the United Kingdom's intelligence services bill was being debated. While the baroness is speaking to an amendment, her comments are applicable to the bill as a whole—and I would like to quote from that *Hansard*:

The noble Baroness said:—

and can you imagine the Australian *Hansard* saying that about any of us?—

The whole point of setting up a special parliamentary committee is to make the work of the intelligence and security services more accountable. Accountability to Parliament is necessary because, first, agents of the state who act on its behalf must be subject to adequate control by the elected representatives of the people. Secondly, the three services must be accountable to ensure that the quite considerable sums of public money spent on them are efficiently and effectively used and not wasted. I regret to say that secrecy can easily encourage inefficiency.

Thirdly, decisions about invading the privacy of others and acting outside the civil and criminal law should not be made by people who have a monopoly of information, who know that they need not share their knowledge and who thus have power without responsibility. Fourthly, accountability and openness can promote public trust and understanding of the reasons for the need to have services of this kind.

I do not believe I have a reputation for being an extremist in the field of human rights, but the third point she makes is vitally important. It is as relevant in the United Kingdom as it is in Australia, and I will read that again:

... decisions about invading the privacy of others and acting outside the civil and criminal law should not be made by people who have a monopoly of information, who know that they need not share their knowledge and who thus have power without responsibility.

One final point: community attitudes towards the intelligence agencies have changed enormously with the ending of the Cold War. There is now no sizeable section of the Australian community believing that there is an instrument of state dedicated to their destruction, in the way that there was through the height of the Cold War. The community expect that we do have efficient and effective intelligence services, and they want to know that they are operating that way.

At this point I would like to make an assessment of where Australia stands in relation to comparable Western democracies. With the possible exception of France, Australia has the lowest level of parliamentary scrutiny of its agencies of any comparable democracy. Denmark, Canada and New Zealand all better our efforts—even Israel. The Knesset's oversight of Mossad, one of the most secretive and effective and, possibly, feared agencies in the world, is far more invigilated by the Knesset than anything in Australia. Germany, probably as a result of the Third Reich experience under Hitler, keeps very tight tabs on its agencies, while Britain and the United States have oversight to a degree that some of our senior public servants either cannot comprehend or, if they do, they will have no part of it. Why is it that all these countries can find some solution to a problem that we will not tackle?

I do not support the US model and I do not want to take time dissecting it here—I would be happy to take questions on that—but I do not see it as a suitable model for Australia. I see the valid model for Australia being in the United Kingdom mould. It may come as a surprise to some members of this committee to realise that the British government up to very recent times never admitted it had intelligence agencies. Despite all the novels about Ian Fleming and James Bond and going right back to John Buchan and *Greenmantle* and all the rest of it, they never ever admitted to having an intelligence agency—and this was a great thing for the government because, if you do not have an agency, then you do not have to have an oversight facility.

But during the latter years of the Thatcher regime, a great debate took place—not in the parliament, but amongst senior public servants in Whitehall—known as the 'debate of avowal'. It was whether Britain should avow—that is, confess—that it had intelligence agencies or should continue to deny them. The avowalists won the argument, with the upshot that in 1994 the Intelligence and Security Committee was set up, comprising nine members drawn from both the House of Commons and the Lords.

I will give a few brief points about that committee. It is a Prime Minister's committee, not a parliamentary committee. In other words, the Prime Minister selects the members, and they are all mature, experienced parliamentarians and they are answerable to him. He has the right to hire; he has the right to fire. The committee members all have unrestricted security clearances and are tightly bound by the official secrets act, or whatever it is in the United Kingdom. Clause 10 of the Intelligence Services Act is a masterpiece of British understatement. The opening part of it says:

(1) There shall be a Committee, to be known as the Intelligence and Security Committee and in this section referred to as “the Committee”, to examine the expenditure, administration and policy of—

- (a) the Security Service,
- (b) the Intelligence Service; and
- (c) CGHQ.

(2) The Committee shall consist of nine members—

Then it goes on briefly. But the essence of this is that the role of the committee is defined in one line: ‘to examine the expenditure, administration and policy’.

There is a final point I wanted to make in relation to parliamentary committees. I may well be wrong in this, but I am not aware of any leak anywhere in any parliament, from a parliamentary committee, which infringed security. Most of the leaks that come in relation to intelligence agencies come from disaffected members of those organisations.

Let us be frank about this. Effective oversight and accountability of intelligence agencies is one of the most difficult tasks a democratic government faces, and that is why I think we have run away from it. But it is not an impossible task. It is very different from bringing other departments of state and their agencies to account. In some agencies, lives are at risk. In all cases the security of the nation is involved. The parliament must approach this issue with the utmost responsibility, balancing the right of the public to know against the very real need for secrecy.

Governments only have two paths to follow here. They either deny any effective accountability process of the parliament, which is the present and proposed course of action, or delegate the responsibility to a select few in the parliament. That is the inevitable compromise that has to be made, and there is no running away from it. Such a proposal is not so revolutionary as it sounds at first. For example, no senator attends every estimates hearing for every department. They are quite happy to delegate that oversight to their colleagues. This provides a working pattern here for the delegation of oversight to a select committee, albeit with the very important difference that that select committee will not, and cannot, report fully on its activities to the parliament and therefore the public.

The need for secrecy is paramount and cannot be compromised. Since it cannot be compromised, it means that every member of the committee must be able to satisfy the requirements of a security clearance at an appropriate level. That again raises huge problems within the parliament that we must address. The first issue is the selection of members. In the bill, clause 28 of part 4, schedule 1 part 3, deals with the appointment of members. The wording is identical to that in part 5A of the ASIO Act, the only variation being the stipulation about government members—which is irrelevant to my point.

This provides for the standard parliamentary practice: the party room selects the party nominees for the committee. Such an approach is totally unacceptable where the sole credentials for appointment are either popularity in the party room or, in the extreme case, just finding someone to fill a committee vacancy. It is quite impossible to put the onus on the party room to

vouch for the suitability of any one of their members with respect to a security clearance. Just think how intolerable it would be if someone were appointed and had to resign because they failed to get clearance. You just cannot do those sorts of things. There has to be another way.

The solution to this problem lies in making a literal interpretation of subclauses 14(1) and (2) in schedule 1, part 3, of the bill, which read:

(1) The members who are members of the House of Representatives must be appointed by resolution of the House on the nomination of the Prime Minister.

(2) Before nominating the members, the Prime Minister must consult with the Leader of each recognised political party ...

And the same should apply in the Senate. In other words, the onus rests with the Prime Minister to nominate members to the committee who will be suitable. He hires and he fires. I recognise that is a compromise on what I said earlier about the independence of the parliament from the executive government, but it is one compromise in this that is inevitable.

All prime ministers have had long service in the parliament before they come to office. They do know a fair bit about their colleagues across party lines and, most importantly, they have access to external advice. In the selection of members there must be genuine consultation with the other leaders in complete privacy. When that is done, a formal approach for a security clearance can be undertaken. That leads to the second huge problem: it is tradition in our parliament that no senator or member applies for or is granted a security clearance. I know that personally from having made many attempts over the years. It would have been of great convenience to me in my work in Defence.

There seem to be different reasons given why we do not give security clearances to MPs and they seem to boil down to two variants of an argument. The first is that the electorate will pass judgment on members and senators who are a security risk and speedily remove them at the next election. I think that is a bit optimistic. The other one seems to be that somehow or other members of parliament are above all that sort of stuff. I have never been able to get an answer that was not nonsensical to why we cannot have clearance. I do not know the best way of tackling this problem. I suspect the problem should be: what level of clearance is appropriate? It may be that there is no level of clearance that is appropriate.

Since leaving the Senate I have been through what I think has been the highest level of vetting for a security clearance. It is a most exhaustive and exhausting process. I do not complain about it, but those of you sitting around that table might reflect in those rare idle moments that you have what is involved when you have to account for pretty well every minute and every dollar you have acquired in a full life. I really wonder whether that level of investigation is necessary for a parliamentary committee. My proposal would be to consult with ASIO and instruct them to come up with an answer. The irony in all of this is that the Minister for Defence, the Prime Minister, the Attorney-General and the Minister for Foreign Affairs walk straight into office when they are sworn in without anyone looking at their backgrounds.

Why all this emphasis on security? Very simply, unless the agencies have confidence in the integrity of every member of the committee, then no meaningful association or interchange will occur between the two. Without a formal assessment, no agency can vouch for the members of a

committee any more than a psychiatrist standing on a street corner can psychoanalyse the crowd walking by. It is impossible to get around the requirement for some adequate vetting process, because only one defaulter will paralyse the committee and thereby render parliamentary accountability impossible. By the same token, it is also mandatory that members of the committee be signed up to the same legal penalties for unauthorised release of information that everyone else is subject to.

A minor problem we have is the Public Service. There is an element in the Public Service in the senior echelons—and I stress it is a minority group—who do not believe in sharing any information with the parliament. This is often associated with the inference that they and they alone can be trusted with state secrets and that no parliamentarian can. This, of course, is basic self-interest. Knowledge is power, and they are not about to dilute their power base by sharing knowledge. I emphasise that that is a minority view, but it is one of the difficulties in getting reform in this area.

I will now turn very briefly to the functions of the committee. The current ASIO committee is ineffectual because the law makes it so. It cannot get involved in anything relating to the core activities of ASIO. In 10 years it has conducted two inquiries—one completed and quite trivial and the other abandoned and also quite trivial—and neither related to the essential business of ASIO. Regrettably, the current bill, while using different wording, does not effectively change the situation.

The inclusion in part 4, clause 30 of a facility to invite the directors of ASIO and ASIS and the Inspector-General to address it merely validates what has been practised in recent years. With the exception of the Director of ASIS, I never experienced any difficulty in getting those people to attend a committee hearing, and they were extremely cooperative. The problem was that the bill gagged them saying anything of any meaning. Two points stand out in relation to the new bill. Clause 29(1)(a) reads:

to review the administration and expenditure of ASIO and ASIS, including the annual financial statements of ASIO and ASIS;

The meaning of that is clear—it is just very plain English. But how will the Chinese Wall be constructed when the committee wants to relate the expenditure to items of administration and not get involved in operational practices? If in doubt, turn to clause 29(3). That is simply a more verbose rendering of what is said in the current ASIO Act. Clause 3 (b), (c), (d), (e) and (g) effectively and totally emasculate any powers of accountability from the committee. Go to the start of it—clause 3, ‘Definitions’. There is no definition at all of ‘administration’ or ‘expenditure’, but the definition of ‘operationally sensitive information’ takes three subclauses and can be interpreted to put a security blanket about anything that a minister wishes.

I think it is highly desirable that current operations are beyond the committee, and that condition must be mandatory. However, an essential part of the accountability process includes an assessment of performance and effectiveness of the agency, and that is impossible without looking at past operations. Furthermore, any review of financial expenditure must be related to operational activities. No meaningful accountability can occur in a vacuum.

The final part I wish to refer to is the exclusion of the majority of the intelligence agencies from token oversight proposals. I can understand the argument that the two included are those which are most sensitive to human rights abuses, but they are also the only two where breaches of security could put human lives at risk. If the government is motivated by a desire to bring accountability to the parliament, it cannot argue that the three left are more sensitive to leaks than ASIO or ASIS—it is simply not true.

I defy anyone in this room to go through the Defence Signals Directorate and learn a thing. It is such an extremely highly technical organisation that the risk of parliamentary oversight is minimal in relation to leaks there. It is very important that the parliament knows something about DSD, because it is operating in an extremely high technology area and its task gets harder on a daily basis. It therefore needs funding at an increasing level to stay competitive, and it will not be supported by the parliament in that unless some information above what is available at the present time comes out about the importance of its activities. The second reading speech says that it is adequately covered at the present time by the surveillance at the Senate estimates committee and by the Senate foreign affairs and defence committee. That is blatantly untrue, as anyone knows. The entry in the budget papers is a one-line entry for DSD, and any minister at the table quite properly refuses to answer any questions at an estimates hearing about it.

The other intelligence agency in the military sphere is the Defence Intelligence Organisation. DIO is a collection agency; it is not a field agency. It compiles military intelligence. There is no reason at all why it could not be part of an oversight umbrella by a parliamentary committee.

The third one is ONA. ONA was established under its own act in 1977 under the Fraser government. Conceptually it is a very good idea, insofar as it collates the intelligence product from the other agencies and fuses it into a coherent stream and provides it to government. In practice it is the most secretive of all. I am not aware of any Prime Minister who has had responsibility for this agency ever being asked a question about it in the parliament. I may be wrong on that, but I am not aware. I am not aware of any representative of ONA ever appearing before a committee. True, the product it is handling is highly sensitive, but the way it goes about handling it is not secretive at all. Again, it is something that the parliament should have oversight of.

In conclusion, what are the arguments that can be put up against this? The first thing that people say is that unnecessary risks are being run by breaking the age-old security maxim of the 'need to know'. I would argue that on a restricted basis the need to know is the valid reason for supporting, not opposing, a parliamentary committee. The second criticism is that all of the organisations are overworked and if you intrude a parliamentary committee into their activities you will substantially reduce their productivity. I do not believe that for one moment. Furthermore, in my discussions with the heads of agencies in the past no-one ever raised that issue with me. In fact, I have not met one agency head who did not support effective parliamentary oversight along the lines that I have proposed.

The final criticism that is often made about increasing surveillance is that no Prime Minister, irrespective of party, would tolerate the leakage of information of current operations to an opposition. That is impossible, because current operations would be withheld from all members of the committee. Furthermore, under existing legislation the Leader of the Opposition can call for a briefing on ASIO at any time, and I doubt that a request for a brief in any other area would

be denied. The more important thing is that such an assertion denies any professional attributes to the members of the committee. There are members of this parliament who would honour the obligations of membership of this committee and conform to them. I am sorry I have taken so long, but I have put a lot of thought into this over the years.

**CHAIR**—Thank you very much, indeed. From what you are saying, does it really matter if this committee and this legislation do not go ahead? Will anything change if they do?

**Dr MacGibbon**—It is not for me to presume to have the impertinence to tell the committee what to do, but I would muse aloud on this. Either you form recommendations from the evidence given by witnesses before this committee which significantly change the legislation or you do not. The response of the government if you do propose change can only go two ways: either they gracefully accept it, and they might, or they reject it. If they reject it, it then goes to the parliament. It either passes the parliament or fails in the Senate. If it passes the parliament I think we face at least 15 years before the bill is revisited. That is the way things go around here. There will be other higher priorities. So we will go for about 115 to 120 years without any parliamentary oversight of intelligence agencies.

Conversely, if the bill is not amended and it is defeated in the Senate then I think the pressures after a face-saving interval of 12 to 15 months, 18 months, would be such that the government of the day, whatever it was, would be forced to come back to the Samuels committee findings of 1994-95 and bring up another bill. I feel strongly that the proposed legislation is inadequate. I want to see change there, but it is really of no moment to me if we wait another two years. We have waited for 100 years already. I do not want to wait for 120.

**CHAIR**—You also referred to clauses that you claim nullify expenditure and administration for which this committee would be responsible. What is your definition of ‘administration’?

**Dr MacGibbon**—You have to find out what the committee is doing in a broad sense. There is no need to go into the fine detail of where and who is the subject for investigation or anything like that, but unless you have an understanding of what that agency is doing in some detail you cannot make an estimate as to what funding requirements that agency needs. That is just not possible.

**CHAIR**—That has always been the problem in the UK—that is, how far you can go in terms of some of that investigation. In the UK, allegedly, they do not get involved in the operations, but as I understand it they often do, because they have to follow these paths in terms of administration and expenditure to find out what the devil is going on. I understand also that there is no real mechanism in their system to solve an impasse when you get there. You may be following a line of questioning about expenditure or planning down an operational route, and all of a sudden the representative of the agency might say, ‘That’s it; I can go no further.’ What happens in a case like that? Should the committee be able to go to another person—say, the Inspector-General or the minister—to get the okay to continue that line of questioning?

**Dr MacGibbon**—You could do all those things, but at the end of the day you would probably have to accept the situation. I would like to go back to the start of your question. I do not believe that a committee of this nature, with respect to its operations, can be codified in words and put into a bill. As the previous speaker said, we are looking at incremental development.

We have no effective oversight at the moment. It would be absolutely unreal to imagine that by passing a bill overnight we would have an efficient set of operating procedures for a committee to follow. That is not the real world. There would be incremental growth. It would probably be five years—two parliaments—before we got effective oversight machinery in place. The important thing is to open the gateway so that we can go down that path.

Going back to the business of codification, I do not believe that you can define. That is why I read that bit about clause 10 from the British Intelligence Services Act 1944. You must have a bit of elbow room. Those few words ‘to examine the expenditure, administration and policy of’ seem to me to encompass very great legislative virtue from an oversight point of view. It allows conventions to be developed. We could have a general rule that current operations are off limits, but we will just go down that path without being bound and constrained the way we are under section 5(a) of the ASIS act and under the relevant sections of the bill.

**Senator SANDY MACDONALD**—Was it ‘policy of’ or ‘activities of’?

**Dr MacGibbon**—It was ‘policy of’. Define ‘policy’ for me. It an amorphous word.

**Senator SANDY MACDONALD**—Samuels recommended activities.

**Dr MacGibbon**—If you wish to debate the Samuels inquiry, we will take the rest of the afternoon. The Samuels inquiry is very interesting, particularly the government’s speech in response to it. I would love to explore that, but, with respect, it is not germane to a critique of the bill.

**Mr BRERETON**—You mentioned that you do not support the US model for security and intelligence oversight. Would you care to elaborate on that?

**Dr MacGibbon**—It is enormous. I do not have much experience of the House of Representatives intelligence committee, but over the years I have had some experience of the Senate one. As you go into the Dirksen building, the entrance to the committee office has armed guards on it. It takes two full floors. As far as I can determine, there is only one entrance which is on the first floor and it has an internal staircase. It is full of people and equipment. It is vast. The chairman is briefed on a daily basis, down to the names of operatives involved in operations. I do not really see the need for that. It operates a two-tiered system. In other words, the chairman is briefed, but the committee may not be briefed. However, the extent of briefings for the committee is beyond anyone’s imagination here. It is enormously intensive. I do not see that that is necessary for the oversight provisions in our circumstances. Perhaps we will go that way in 50 years, but initially I do not see that that is the case. That is my objection to the American system. If anyone proposed the American model, you would really be overvolking the custard.

**Mr BRERETON**—How do they address the security clearance issues?

**Dr MacGibbon**—I do not know how they get over that. They have a rotational system. They will not permit a senator to stay for longer than the statutory period of six years, or something like that, so that they are not captives of the organisations philosophically. They rotate them through. They have a reasonably large pool to draw from, so I suppose that they can do that.

To diverge for a moment, Tom King was the first chairman of the United Kingdom committee and I knew him reasonably well. I remember having lunch with him one day in the House of Commons and I said, ‘Tom, with only nine members and 685 members in the House of Commons and about the same number in the House of Lords, it would be a bit of a luxury for you to just pick only nine out of about 1,200-odd candidates.’ He said, ‘That’s not true. It is difficult to find nine suitable members for our committee.’ The point is that you need people with experience and maturity. You do not want the extremists on it. You have to have people who can satisfy a security clearance. You have to have people who are not publicity seekers, which is a rare event for members of parliament. You cannot hold a press conference after you have had a committee meeting. That narrows the group down. The Americans seem to get by with that.

**Mr ANDREWS**—To summarise your argument, David, it involves two propositions: first, that the oversight committee must be able to review the past operations of the security services, and secondly, in order to achieve that, consequently the members of the committee must have security clearances for that to occur properly. If that is right and we were to accept your argument, could that not be achieved in the bill by simply doing two things—firstly, by removing the words, ‘that have been’ in clause 29(3)(c) so it is clear that the committee would not be excluded from reviewing particular operations that are past; and secondly by adding to the bill a provision or at least the regulations that might be made pursuant to the bill, or at least the operation in some way, in respect of the provision about security clearance?

**Dr MacGibbon**—On your first point about looking at past operations, I would not see it as an entitlement of the committee to go into detail. We are dealing with generalities here. The committee ought to know the nature of past operations and what the outcomes were and that sort of thing. I do not think that it would be proper for it to probe into minute detail as to what went on and that is a convention that the committee could develop. As for your suggestions, maybe they will work. On the run, I do not know about that. You have to get a pathway through a very real human problem, which is getting people who satisfy a security clearance through the parliament. It is a real problem. You just cannot call for nominations for the committee, put up people’s names and have them knocked out. You cannot do that to them.

**Senator ROBERT RAY**—Can you think of one person in the parliament who lacks the pride to refuse the security clearance process, knowing that the foreign minister, the defence minister and the Attorney-General do not go through the same process? It goes against human nature. I am not going to put myself up for a security clearance to run for one of these committees. I am just not going to do it, no matter what my background is, knowing that the people with their hands on day-to-day operations do not go through that. It defies political pride—that is the problem. I can see the logic of your argument, because you want to have a proper process of scrutiny; I acknowledge that. But I do not think we should pay the price by saying, ‘Yes, we will get a security clearance,’ but A, B and C do not have to. I cannot understand that.

**Dr MacGibbon**—That is one of the compromises I am prepared to make. You are not.

**Mr LEO McLEAY**—But isn’t it restrictive enough if the Prime Minister appoints the people?

**Dr MacGibbon**—I do not wish to comment on that. I will pass on that one.

**Senator ROBERT RAY**—But you have commented that you think prime ministers are in the best place to appoint members of this committee. That seems to me massively politically naive, given the penchant of prime ministers of either persuasion for cronyism. It comes with the job. It is something you pick up the day after you get the job. Prime ministers appoint people in this order: they appoint their enemies first to positions, to keep them out of the road; they then appoint their friends; and ability usually comes third. That is human nature.

**Senator FAULKNER**—That is a bit rough, because most prime ministers made that an art form well before they were elected to that office.

**Dr MacGibbon**—Let me give you the facts of life, Senator Ray. If you follow the course that you are advocating, you will not have effective accountability by a parliamentary committee. I do not care what act you pass or how precisely you spell out the powers of the committee—no director of an agency will compromise the security of that agency before a committee that they have question marks about at the back of their mind. They cannot pick the credentials of members of a committee just by looking at their faces. They have got to have a process that is codified by which they can—

**Mr LEO McLEAY**—What do they do with their minister then?

**Dr MacGibbon**—I have not been in that position, so I cannot answer it.

**Mr LEO McLEAY**—Doesn't that knock your argument down? If you say these characters are going to be not quite frank with the committee because they do not trust the background of the committee member, if they did not trust the background of the minister, then, by the same logic, they would not be frank with the minister.

**Dr MacGibbon**—They may or may not have been in the past.

**Senator ROBERT RAY**—In fact it is a psychological thing. They are trained to accept the minister. Do not think I am disagreeing with your method of appointing the committee members. The other side has just as many downsides. I just thought that there was a touching naivety about the trust in the Prime Minister. I would have thought the real responsibility is on the Prime Minister. If he makes a mistake it is his mistake, and he bears it all the way through politically.

**Dr MacGibbon**—That is precisely what I am getting at. He carries the can for this. It is on his head that Bill Jones was appointed and, by appointing him, he is vouching for his integrity. If he has not taken covert advice as to the suitability of Bill Jones for that job, he is going to face up to the consequences.

**Senator FAULKNER**—But you suggest also that the Prime Minister appoints opposition members to the committee after consultation with the Leader of the Opposition.

**Dr MacGibbon**—But, like a vacancy in the Senate, the Prime Minister does not select. He consults, and the Leader of the Opposition—or the leader of another party—gives him a list and says, 'These are the people', and the Prime Minister accepts those, provided they are clearable for a security clearance.

**Mr MELHAM**—But what are the criteria? I have got a background as being in the Left of the party, as well as a legal aid background and a public defenders background.

**Senator ROBERT RAY**—Don't apologise.

**Mr MELHAM**—I am not apologising. I have got a healthy cynicism when it comes to prosecution authorities and those that operate behind closed doors. Is that a disqualification for appointment to a particular committee such as this?

**Dr MacGibbon**—No, I do not agree with that.

**Mr MELHAM**—That is what worries me about having to be subject to prime ministerial approval or veto before you can be appointed, because there are some prejudices that do flow with that.

**Dr MacGibbon**—I do not know your private life, so I cannot comment on it, but I would be surprised if, from what you have said today, you would be debarred, censured or prejudiced in any way at all for a clearance.

**Mr LEO McLEAY**—The most depressing thing for Daryl was that he applied for his ASIO file under FOI and they did not have one.

**Mr MELHAM**—If only it were true.

**Senator FAULKNER**—Let us be clear about this: you are saying in relation to the appointment of opposition members to the committee that there is no right of prime ministerial veto over the Leader of the Opposition's nominees.

**Dr MacGibbon**—That is what I am driving at.

**Senator FAULKNER**—You are saying that, under your model, the only veto goes to whether or not government or non-government nominees are able to obtain a security clearance. I think that is what you are saying.

**Dr MacGibbon**—Correct. That is what I am saying.

**Senator FAULKNER**—So under your model, if there were three members of the opposition to serve on such a committee—let us pick a number out of the air—and the Leader of the Opposition provided three names to the Prime Minister, the only veto that could be applied would be failure to obtain a security clearance.

**Dr MacGibbon**—Quite. Don't you agree with that?

**Senator ROBERT RAY**—Do you remember who gave the security clearance for Aldrich Ames, the FBI bloke who has just pleaded guilty and will get the death penalty? I am not as convinced on security clearances as you are, frankly. I am convinced with people's honour.

**Dr MacGibbon**—No. I am not convinced on their accuracy as a guarantee, but you tell me another substitute that takes their place. In the absence of an alternative, they are the only recourse you have. We had a very unfortunate incident in this country in the last 24 months about somebody granted clearance in the United States. While you brought the subject up, I do not want to dwell on mistakes in the agencies, but every so often we do have a public crisis. For every crisis that appears in public, there are more internally that never come out, and you would know that very well as an ex-minister.

I do believe that a parliamentary committee which has some real powers to oversee the operations will in some way reduce the possibility of those crises occurring. You cannot get into that depth unless the committee has the credentials to establish their bona fides. That is what I am labouring over. I do not know how you get the confidence of the agencies, unless you meet the standards that they impose on themselves. I think that is the best way of putting it.

**Senator ROBERT RAY**—You were in fact wrong before when you said that ONA have not been subject to questioning, to Senator Faulkner's and my bitter disappointment. We have examined them, but admittedly not too rigorously. The alternative is to bring about what you want: for people to start to use the estimates committees and Senate committees to examine these agencies in a lot more depth than they have in the past. That is an alternative I do not think the agencies would want. They would much prefer a specific committee, as you say, brought up in the traditions of the whole security area and understanding its nuances to do it rather than letting a thousand flowers bloom through the Senate estimates process.

**Senator FAULKNER**—Even though I believe in the accountability mechanisms of the parliament, I think you might have been suggesting earlier in your statement that the best accountability mechanisms of the parliament at the moment happen to be in the Senate legislation committee processes. Nevertheless, there is a tremendous weakness, isn't there, in the capacity for members of the House of Representatives—with a much bigger pool of talent, if you like, with double the number of parliamentarians to draw on—to fulfil this important role? Basically they are excluded from that level of scrutiny.

**Dr MacGibbon**—That reinforces the case for a joint committee.

**Senator FAULKNER**—In relation to the estimates processes, is that a concern that you have?

**Dr MacGibbon**—Yes. And one of the other problems with the estimates committees is that, by regulation of the Senate, they must always be public hearings; they cannot go in camera. It is quite proper that that should be so. But that cannot work for an intelligence agency. But to come back to the point you are making: yes, the presence of a joint parliamentary committee would allow the House of Representatives to have meaningful input that is denied them at present.

**Senator ROBERT RAY**—There are two issues here: coverage and depth of powers. This bill will expand coverage by one but will not really increase the depth of powers of scrutiny at all.

**Dr MacGibbon**—Yes.

**Senator ROBERT RAY**—Wouldn't one possible starting point be to increase the coverage—cover DSD, cover DIO, cover DIGO and cover ONA—so that all six agencies are covered and, then, as the committee builds up its gravitas and depth of experience you move to an extension of powers? That at least would be a step forward if we went that way in our recommendations.

**Dr MacGibbon**—It would undeniably be a step forward, but I see no logical reason why in this day and age we should not move to effective parliamentary oversight—excepting, of course, that it is going to take time to build it over the years to an effective level. Your process would put us back five or 10 years.

**Senator ROBERT RAY**—I would not have thought it was that much.

**CHAIR**—As there are no further questions, thank you very much, David, for a very pleasant hour and a quarter.

**Dr MacGibbon**—Thank you. I forgot to mention one last thing: years ago I drafted a bill on this. You might be interested in it. It is a couple of years out of date but I table it for your consideration.

**CHAIR**—Thank you.

[3.14 p.m.]

**O’GORMAN, Mr Terence Patrick, President, Australian Council for Civil Liberties**

**CHAIR**—Welcome. Although the committee does not require you to give evidence under oath, I should advise you that the hearings are legal proceedings of the parliament and warrant the same respect as proceedings of the House or the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. Do you wish to make some introductory remarks before we go on with questioning?

**Mr O’Gorman**—Yes. Dr MacGibbon has spent his time giving a detailed critique of the inadequacy of the powers of committee oversight. Let me direct members of the committee to those comments I make at pages 1 and 2 of my submission and particularly to an article from the *Nation* publication in the US, which indicates in effect that the detailed provision of operational information to congressional oversight committees in the US works. It seems to work well and it brings forth transgressions of the CIA in particular, which, as I understand it, is the closest US intelligence agency to ASIS. It brings them out into the light of day, and I submit that it brings them out into the light of day because those committee members are in fact briefed in some apparent considerable detail. Indeed, I listened with interest to what Dr MacGibbon said in that regard. His objection to that detailed provision of operational information seems to be a resource one rather than a philosophical one. My view, without being a slavish follower of US procedures, is that if it works well in a country of that size—in a country that is a much bigger player in the international intelligence services scene—why can’t it work here?

I will move on to other things. Section 11(2) of the bill says that ASIS functions do not include the carrying out of police functions or any other responsibility for the enforcement of the law but in other sections, in my submission, it goes on to provide for exactly that. I would like to go directly to page 8 of my submission in case I run out of time. There is a provision in the bill that gives ASIS the power to gather criminal intelligence overseas including, as I read it, on Australian citizens and to pass on that criminal intelligence—I stress I am talking about criminal intelligence, not national security intelligence—to domestic law enforcement agencies for their use. I want to concentrate primarily on that, and if there is time I can go back to other aspects of the submission. Page 8 of my submission, under the heading ‘Liability for certain acts’, says:

Section 14 provides that a person—

in ASIS or DSD—

is not subject to any civil or criminal liability for an act done inside Australia if the act is preparatory to, in support of or otherwise directly connected with overseas activities of the agency concerned.

Nowhere in the second reading speech is there any reference to this. You have to dig about the act. Fortunately there is some honesty in those who prepare the explanatory memorandum, because there is some reference to this in the explanatory memorandum but nowhere in the second reading speech. I will read it again:

Section 14 provides that a person—

—for ‘a person’, read an ASIS or DSD operative—

is not subject to any civil or criminal liability for an act done inside Australia if the act is preparatory to, in support of or otherwise directly connected with overseas activities of the agency concerned.

The statement in the explanatory memorandum contends that the purpose of this clause is to provide immunity in a limited range of circumstances for activities carried out in Australia by ASIS that have a connection with some overseas activities by ASIS. I contend that the explanatory memorandum argument that this provides only a limited range of circumstances for ASIS and DSD to break the law in Australia is simply not right; it is much greater than limited. The term ‘preparatory’ in ordinary criminal law has been given a very wide definition indeed.

**Mr MELHAM**—How would you limit it to Australia? What words would you use to have the limited effect that the explanatory memorandum suggests? Do you have any substitute words that you would put in?

**Mr O’Gorman**—Not yet, but I might, as a result of participating in this committee, including staying around for tomorrow. I do not know that it is properly understood that in this bill ASIS is being given the role to collect criminal intelligence overseas and make it available to domestic law enforcement agencies, and ASIS and DSD in Australia can break Australian domestic law if it is ‘in support of’, ‘preparatory to’ or ‘otherwise directly connected with’ what ASIS is doing overseas. So I respectfully urge committee members to have a look at those phrases, including ‘otherwise directly connected with’.

My contention is that those phrases would enable ASIS and DSD to engage in very significant criminal activity within Australia—that is, activity which breaks the criminal law—so long as they can show that such activity was ‘connected with’—and those very wide phrases I have referred to—the overseas activities.

**Senator ROBERT RAY**—You may be going on to acknowledge this, but the Inspector-General can review every one of these files.

**Mr O’Gorman**—Yes, and I have a concern about that. That raises the question that the chairman asked of Dr MacGibbon. Dr MacGibbon was talking about the UK committee where they ask much more detailed questions. An operative could then say, ‘I am not going to go any further, because I will reveal sensitive information.’ The reality is that, unless you can do something to break that refusal by the operative to go any further, you just do not get the information.

**Senator ROBERT RAY**—I am sorry, but those operatives and those agencies, including the one we are looking at today, do not have that right to refuse the Inspector-General at all.

**Mr O’Gorman**—No, they do not have the right to refuse the Inspector-General.

**Senator ROBERT RAY**—The Inspector-General can go through the files, do interviews and do everything. I am not deflecting your main point, but there is a level of scrutiny when you want to take it to the extremes, which you are doing at the moment. It is discoverable.

**Mr O’Gorman**—I am going on to argue on the rest of page 9 about the use in a subsequent criminal trial of criminal intelligence information that has been obtained by ASIS.

**Senator ROBERT RAY**—But it cannot be.

**Mr O’Gorman**—Why not?

**Senator ROBERT RAY**—Nothing that ASIS collects can be used in a criminal case. It can only alert the authorities.

**Mr O’KEEFE**—This is where I think you have drawn too long a bow. I have not seen any wording that takes us where you have taken us. You have looked at both the second reading speech and proposed section 14 of the bill, but have you read them together? Proposed section 14 relates to the proper performance of the function of the agency and the second reading speech says:

Immunity will only be provided in respect of activities carried out in accordance with the directions issued by ministers.

Assuming that any court will read both the act and the intent of the act, do you not agree that those specific conditions would have to be demonstrated to have been met? Do you think you can draw it further than that? I think that is what you are doing; you are drawing a longer bow than that.

**Mr O’Gorman**—No, I do not think I am. I am making the point that, if ASIS gathers criminal intelligence and that criminal intelligence is in some respects false, it passes it on to a domestic law enforcement agency and it is used in the prosecution of an individual—

**Senator ROBERT RAY**—It cannot be.

**Mr O’Gorman**—It cannot be directly used, but it can be given to, say, the AFP or the NCA and they can then run off that criminal intelligence that DSD or ASIS has gathered and use it—not directly but in a derivative sense—to mount a criminal prosecution—

**Senator ROBERT RAY**—It is in an alert sense. It can alert them. This does not necessarily detract from some the points you are making, but we are just trying to get precision, you understand. Generally, this information is incidental, because it is not particularly being targeted. It can go to domestic agencies to alert them to the problem. The material they gather cannot be used in a court case; it can only alert the Federal Police and so on that, for example, there is a people smuggling operation about to start here, there or anywhere. They have to then gather evidence and prosecute. They cannot use the ASIS material in a court of law.

**Mr O’Gorman**—They cannot use it directly in a court of law, but it can be used as part of the investigative pattern, the investigative materials that are eventually used in a court of law.

**Senator ROBERT RAY**—It can stimulate the investigative pattern. There is no doubt about that. You may object to that as well—I do not know—but it can certainly do that.

**Mr O’Gorman**—My concern is that it can do more than stimulate it. As I read these provisions, ASIS can—without the protection of a judicial warrant—tap the phones of, say, Australians overseas for the purpose of gathering criminal intelligence and then pass the product of that on to, say, the AFP or the NCA, which can then in due course mount an operation against that target. It may be that there could be some material in ASIS gathered criminal intelligence which, if it was known to the defence in a criminal trial later on, could be relied upon to show that the prosecution’s case is not what the prosecution are claiming it to be. In other words, it could be used by the defence, if it was able to get hold of that first step criminal intelligence, to argue that part of the prosecution’s case against their client is fabricated. That is my concern.

**Mr BRERETON**—You are making this point in an area which has nothing necessarily to do with security. You are making it in respect of criminal behaviour, potentially, by Australians citizens out of the country.

**Mr O’Gorman**—Yes, and my concern is that this provision that gives ASIS the power to gather criminal intelligence overseas reflects what happened with MI5 and MI6 after the end of the Cold War. They, according to one view, had lost a large area of their ordinary area of operations so they then wanted to move into, effectively, domestic policing. There was then a turf war fought between them and the ordinary law enforcement agencies in the UK. My concern is that this is an Australian version of what happened with MI5 and MI6. I readily acknowledge what Senator Ray says, that illegal telephone tapping done by ASIS of an Australian citizen overseas cannot be directly used in a later criminal trial, but it can be given to the AFP or the NCA, which can then mount an operation and eventually a person is put into court. They are not put into court on the direct evidence of what ASIS has gathered, but it may be that some foul play has surrounded the gathering of the initial intelligence and under the provisions of this act none of that contaminated evidence that ASIS has gathered—whether it has done the contamination or someone else has and it has picked it up—will find its way into court.

**Senator ROBERT RAY**—But none of this material can find its way anywhere, because the Inspector-General, when he realises that an Australian citizen has been a target specifically overseas, is going to rule out the use of the material. We are looking at a dodgy analogy; we will have to find another one that suits the purposes. ASIS cannot go overseas, as I understand it, and target an Australia citizen. Their dilemma is, when they gather information overseas and it has incidental reference to Australians, whether or not they can even use that. That is usually where the pivotal area is. They cannot go overseas and target an Australian citizen.

**Mr O’KEEFE**—To take a different analogy, it is a common courtroom practice for a lawyer to ask the police, ‘How did you get onto this bloke?’ and for them to answer, ‘We got an anonymous tip,’ or, ‘We have an informer,’ and the court cannot get any better information than that. It works from the quality of the evidence that has been gathered from that point on: does it pass the evidence test and is it substantial? Nothing that ASIS can provide in a situation like that would be anything more than, basically, the lead tip.

**Mr O’Gorman**—The problem in the ordinary criminal court is that the police can say, ‘Our information came from an informer,’ and that informer, as Fitzgerald and Wood showed, can be corrupt.

**Mr O'KEEFE**—Or mischievous, yes.

**Mr LEO McLEAY**—Isn't that the problem? If ASIS, in pursuing a people smuggling operation, come across a drug operation—some of these people tend to act in concert with each other—and they pass on that information to the AFP, the AFP have to mount their own brief of evidence on material that they acquire in accordance with the law.

**Mr O'Gorman**—Yes.

**Mr LEO McLEAY**—Why does the fact that they were pointed towards the information by ASIS create a problem? How is it different from someone ringing a drug hotline and saying, 'Get a search warrant and search the house next door'?

**Mr O'Gorman**—If the information gathered by ASIS was, say, from their own telephone tap and if the information of that telephone tap were known to the defence and could be put in front of a jury, it may well put a different interpretation on the later telephone tap that the NCA or the AFP mount against that target. In other words, ASIS might have gathered criminal intelligence which, if it were known to the defence that it existed, the defence could use to say, 'This is not what the prosecution evidence would have you, the jury, believe is the case.'

**Senator ROBERT RAY**—Would you argue that they just never pass anything on? They are a secret intelligence service. They are not open to the normal discovery methods. Are you arguing that they should not pass on information if they discover a paedophile ring or a drug offence? Should they not pass it on to the relevant authority?

**Mr O'Gorman**—No, I cannot credibly argue that, but my concern about the bill is that it moves ASIS from a national security focus in its overseas activities and says, 'And while you're there, you can carry out as much criminal intelligence as the minister might direct you to.'

**Mr LEO McLEAY**—How do you draw that conclusion? That is not what the bill says. The bill puts on a statutory basis what the ministerial directive has told them that they have been able to do in the past. It is codifying what they have been able to do in the past. Their major function is to look at intelligence matters, not to look at criminal intelligence matters. Criminal intelligence matters, if they come across them, are a by-product; they are not their major product.

**Mr O'Gorman**—Clause 6(a) says:

(1) The functions of ASIS are:

(a) to obtain, in accordance with the Government's requirements, intelligence about the capabilities, intentions or activities of people or organizations outside Australia ...

**Mr LEO McLEAY**—That is right, and the government gives ASIS a direction on what its priorities are.

**Mr O'Gorman**—But it does not define intelligence to mean national security intelligence. So if you then combine section 6 with section 14, I contend that ASIS can now, for the first

time—as far as we know—gather criminal intelligence outside of Australia. If we go back to clause 6(1)(a), it is in accordance with the government's requirements 'about the capabilities, intentions or activities of people or organisations outside of Australia', including Australian citizens.

**Senator ROBERT RAY**—So what you are really arguing for are the critical points in the minister's directive, of which you and I are not aware—although I probably have a clearer idea than you have simply because of our involvement in this issue. I do not think ASIS wants responsibility for criminal intelligence per se. However, would you accept that neither you nor I can know what the directive is, and that is what you are concerned about? If the directive is too loose, and if it covers these criminal areas, you will be concerned.

**Mr O'Gorman**—That is my concern.

**Senator ROBERT RAY**—We say that there has to be some trust in government—not always, but some trust—that they will restrict the use of ASIS to its proper purposes. There is an amendment about people smuggling because that is regarded almost as a national security issue and we understand that, and we have an Inspector-General to at least make sure that they comply with the directive. If the directive does not include criminal intelligence, they cannot go off on a romp on their own; the Inspector-General would turn that up. It really narrows down to what directions the government gives to ASIS in terms of its operations.

**Mr O'Gorman**—Yes, and my argument is that clause 6 states:

(1) The functions of ASIS are:

(a) to obtain, in accordance with the Government's requirements, intelligence ...

and if you look at the definition section, intelligence is not defined. The government can then tell ASIS to go to criminal intelligence overseas. I am concerned that the defence will not know if there is something in that criminal intelligence which is gathered, which is then passed on to the AFP or the NCA, that contains exculpatory material.

**Senator ROBERT RAY**—I suspect that they have not defined intelligence because they did not want to distinguish between HUMINT and SIGINT. That is why they have not specified that in the act, and not whether it be criminal intelligence or national security intelligence.

**Mr O'Gorman**—While that might be so, my submission is that I am not, in the words of one of the committee members, drawing a long bow when I say that if ASIS is empowered to gather criminal intelligence, even if that is not going to be 90 per cent of its activities, and the criminal intelligence it gathers then leads to a domestic law enforcement agency eventually making an arrest and the ASIS criminal intelligence contains exculpatory information for the accused, where is the machinery for that exculpatory material to be made available to the defence or to be known to a jury? That is my concern. I am concerned that unless IGIS is specifically empowered to, on a defence request—say by way of subpoena—look at ASIS and its intelligence gathering in a particular case to see whether there is something relevant that might be exculpatory to the defence, we are sowing the seeds of a miscarriage of justice.

I want to make the point that I am not saying that ASIS should not gather criminal intelligence. With respect, what Senator Ray says must be correct. While lounging on a beach somewhere in Asia, if ASIS falls upon an Australian paedophile performing paedophilic activities, of course the agent cannot close his mind to it. My concern is—and this is not theoretical—that unless the criminal intelligence that ASIS gathers that stimulates a domestic law enforcement investigation is available at least through the filtering mechanism of IGIS, unless I can deliver a subpoena on behalf of an accused to IGIS to say, ‘I want you, IGIS, to go through some possible criminal intelligence that ASIS might have gathered here because there may be something that could be exculpatory to my client,’ surely if ASIS is going to be given a criminal intelligence role, if we are to avoid miscarriages of justice, there must at least be that sort of amendment.

**Senator ROBERT RAY**—But does not the miscarriage of justice depend on the fluke of whether you know that ASIS at some stage has its fingers in this?

**Mr O’Gorman**—When I am representing someone, if it is on the cards—to use the words of Alistair and the High Court—that ASIS might have been involved, I should be able to direct a subpoena to IGIS to say, ‘You give me what criminal intelligence ASIS gathered on this that may be relevant. It is not for IGIS to decide whether it is relevant to my defence.

**Senator ROBERT RAY**—I follow that, but we would not want to encourage—and I do not think you would—everyone to do that as a standard procedure legal manoeuvre when it might be only one in 5,000 cases.

**Mr O’Gorman**—But with my subpoena to IGIS, I would not necessarily, under my proposal, be compelled to come to court and be cross-examined on what IGIS may have found in the relevant ASIS file. There are protections for public interest immunity, et cetera.

**Senator ROBERT RAY**—I am just concerned that the Inspector-General does not have to respond 300 or 400 times a year to one of these and, in that year, nothing is ever turned up, and it just becomes a delayed procedure or something else.

**Mr O’Gorman**—That is a concern, but I return to my concern that the common ingredient in miscarriages of justice in this country and in the UK is the failure to disclose relevant material held by prosecution agencies. If ASIS is going to be a prosecution agency to the extent of now being empowered to gather criminal intelligence, and you cannot deal with disclosure problems, you are setting up the possibility of miscarriages of justice.

**Senator ROBERT RAY**—But aren’t we going to get the argument going the other way? By the way, I do not disagree with any point you are making about the withholding of evidence. It has been one of the biggest problems we have had. Once you get to the point where it has to be discovered whether there is any evidence that assists in the defence, people will start arguing. But if there is evidence that is pretty much going to sink the defence, that should not congest. Which is something that takes ASIS well outside what anyone wants it to be doing.

**Mr O’Gorman**—I would argue that it need not go that far. All I am directing the committee’s attention to is the necessity—because a failure to comply with the rules of disclosure leads to miscarriages—to address some mechanism of allowing the defence to get access to criminal

intelligence which ASIS might have gathered. I accept it can be abused, but because it can be abused does not mean to say it should not be tried. The police abused the verbal for 20 years. They were not prohibited from doing interviews.

**Senator ROBERT RAY**—It just seems to me that you would have to know, but we are not in a position to know how often this is likely to occur. You would say that if it occurred once, it is once too often. But it may never occur.

**Mr O’Gorman**—The reality is, though, that you would need to have an extraordinarily well resourced, repetitive defence team to be constantly throwing 400 of these subpoenas to IGIS each year. It is just not going to happen.

**Senator ROBERT RAY**—I accept that. What I am now saying is that these circumstances may never have occurred in the past and may not occur in the future.

**Mr O’Gorman**—My contention is: with the express power given to AGIS to gather criminal intelligence, it is now out in the open. Even if they have done it in the past, we have not known it. It is now out in the open, it is statutorily provided for. There has got to be some protection in respect of the concern that I am articulating.

**Senator ROBERT RAY**—But a lot of that collection is done via information gathered. It is not by wire tap or anything else; it is by way of human intelligence. They would need a whole range of protections, I think you would agree, going back into defending that, wouldn’t they—in terms of revealing the names of sources et cetera.

**Mr O’Gorman**—If one were to direct a subpoena to IGIS, IGIS could be empowered to be restrictive in the information it hands over to address those concerns. But at least one ought to be able to go to IGIS to say, ‘We have reason to believe that ASIS might have gathered criminal intelligence,’ to use your paedophile example, ‘and we have reason to believe that there might be some criminal intelligence there that shows that it was someone else other than my client who was observed to lead the child from the beach to the nearby hotel room. We want you, IGIS, to at least examine ASIS’s holdings to see whether there might be some evidence there that might indicate that.’

**Mr O’KEEFE**—But, just to take the analogy further, surely the alleged offence has not even made it to a court unless an authority has gone and got its own evidence. In the analogy you are putting, all ASIS is saying is, ‘Listen, by the way, we were doing this and we happened to notice that this guy picks up boys on the beach.’ But that is not the basis of a case. The Federal Police then have to go and make a case. That case needs to be made by them gathering their own evidence, making their own observations and taking their own photos or whatever. So, unless that was repeated, there is no case. Where you are coming from is much more subtle than that, I am sure. But are we being misled in our understanding of this? In the whole consideration of this, our assumption is that ASIS can play no role in the collection of data for activities other than intelligence. If it comes across incidental information and decides to pass it on to the authorities—which we all agree is fine—nothing can stem from that other than it being the lead that got an investigation going.

**Mr O’Gorman**—On my reading of the act, ASIS can tap phones in Australia without the necessity for—

**Mr LEO McLEAY**—No, in Australia they cannot.

**Mr O’Gorman**—My submission is that section 14(2) will permit that. But perhaps I can make the point and then go back to section 14(2)—

**Mr LEO McLEAY**—You are putting a lot of emphasis on sections 6 and 14 by which you have brought in a few red herrings. But does not section 11, the limits on agencies’ functions, specifically exclude agencies from carrying out any police functions or any other responsibilities for the enforcement of law?

**Mr O’Gorman**—But ‘police functions’ are not defined.

**Mr LEO McLEAY**—It says that the agencies’ functions do not include the carrying out of police functions—

**Mr O’Gorman**—Yes, but ‘police functions’ are not defined, and so police functions could be—

**Mr LEO McLEAY**—or any other responsibilities for the enforcement of law.

**Mr O’Gorman**—‘Police functions’ could be interpreted to mean making an arrest. My argument is that, when you particularly have regard to section 14, section 11 does not say that ASIS cannot gather criminal intelligence.

**Mr LEO McLEAY**—They have not carried out an arrest, as we understand it.

**Mr O’Gorman**—I am not talking about carrying out an arrest. I am saying that section 11 does not prohibit ASIS from gathering criminal—as opposed to national security—intelligence.

**Mr LEO McLEAY**—Section 11(1) says:

The functions of the agencies are to be performed only in the interests of Australia’s national security, Australia’s foreign relations or Australia’s national economic well-being and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.

**Mr O’Gorman**—But national security is not defined and economic wellbeing is not defined. So, if both those terms and ‘police functions’ are not defined, and reading section 11 with section 14, what is there to stop ASIS from gathering criminal intelligence—whether it is 30 per cent of their work or 90 per cent is irrelevant—and then passing it on to domestic law enforcement agencies? If the terms used in section 11 are not defined—

**Mr O’KEEFE**—There is nothing to stop it from occurring. In fact, section (c) of the act provides for intelligence to be passed on.

**Mr O’Gorman**—Yes.

**Mr O'KEEFE**—None of us are trying to mount a case—and you agreed earlier—that they should be prohibited from passing the information on.

**Mr O'Gorman**—No, I am not.

**Mr O'KEEFE**—Where you are coming from is the accountability of the original collection of that information in a subsequent court case.

**Mr O'Gorman**—Yes.

**Mr O'KEEFE**—We have to make a value judgment about the point you raise as against whether it is necessary to go back any further in a court case than the activities of the prosecution bringing forward the case, which must have been mounted on subsequent evidence. Pick a different example.

**Mr O'Gorman**—I will pick a different example.

**Mr O'KEEFE**—Let me give you one. Tell me where you would go with this. Let us say ASIS were, under proper authority, as required in both the second reading speech and the act, investigating some gun runners providing arms to a paramilitary organisation in a country that might threaten our national security and it just happens that birds of a feather flock together and, in the process of checking out the gun runners, they come across people smugglers and drug traffickers and they happen to spot in the middle of all of this an Australian, who was not the subject of the investigation in the first place—none of their activities even incorporated an Australian in the first place. Our understanding of the process from there on is that they might pass that information to the Federal Police or Customs or NCA or whoever and say, 'Have a look at this bloke,' and that is the end of it.

**Mr O'Gorman**—If that was the end of it, it would be unobjectionable. But it need not be the end of it. To use another example, if ASIS in carrying out its work was engaged in phone taps—and I understand it can engage in phone taps without a court warrant—

**Senator ROBERT RAY**—In Australia?

**Mr O'Gorman**—At least outside of Australia, for the purposes of this example.

**Senator ROBERT RAY**—But within Australia it cannot, can it? You said before that it could.

**Mr O'Gorman**—Can I come back to that after I enter this example. Let us say ASIS is tapping an Australian's phone overseas and comes to the conclusion that that information should be passed on to a domestic law enforcement agency and eventually the domestic law enforcement agency mounts its own operation using, say, telephone taps and puts the person in court. If there is something in the ASIS telephone tap which might point to a person's innocence should there not be some machinery for an Australian court to obtain that information? My answer is that there must be, if we are to avoid miscarriages of justice. My submission is that in this act there is no provision for it. To answer Senator Ray's question, my interpretation of subsection 14(2)(a) is that ASIS, as in that example, can tap a phone within Australia if it is

‘preparatory to, in support of, or otherwise directly connected with, overseas activities of’ ASIS at a particular time. My argument is that subsection 14(2)(a) enables ASIS within Australia to tap phones of Australian citizens without judicial warrant if, to use the terms of the act, it is ‘preparatory to, in support of, or otherwise directly connected with’ the activities of ASIS tapping an Australian’s phone overseas.

**Senator ROBERT RAY**—We just know that that does not happen.

**Mr O’Gorman**—How do we know that, with respect?

**Senator ROBERT RAY**—We know that from what we as a committee know.

**Mr O’Gorman**—Well, I do not.

**Senator ROBERT RAY**—You do not, but we at least know that we can rest easy on that one. They do have an ability, as do a whole range of other organisations, to access information as you have described but all via warrant and all via another agency. So that is not a long-term concern for us.

**Mr O’Gorman**—It is a concern for me. If it is not a concern for you, we part company.

**Senator ROBERT RAY**—I am saying it is done by a warrant. You are saying they can do it without a warrant, and we are saying that it is not possible, under instructions from the minister or anybody else. The only way they can do what you are saying they can do is by a legally obtained warrant through a proper statutory base that already exists.

**Mr O’Gorman**—From the Attorney-General, not from the court.

**Senator ROBERT RAY**—Yes, from the Attorney-General, the same as ASIO or anything else.

**Mr O’Gorman**—The problem is that the Australian citizen’s phone is then tapped not by way of a court warrant but by way of an Attorney-General’s warrant. Again, my concern is what if there is information in that telephone tap of the Australian citizen’s phone that is relevant to the defence of the eventual accused.

**Senator ROBERT RAY**—But it has to be within the powers of either ASIO or ASIS, and that is why we have an Inspector-General, why there are specific rules in terms of Australian citizens that he is there to protect. If this ever occurred—and I am saying ‘if’—the Inspector-General would have access to every one of those files.

**Mr O’Gorman**—But how do I get them if I am representing the particular accused?

**Senator ROBERT RAY**—I am sorry; that is another issue.

**Mr O’Gorman**—It is a central issue that I am submitting about.

**Senator ROBERT RAY**—What you are saying is that a defence team should be able to apply if there is some sort of sniff that ASIS has been involved to the I-G. The solution may well be that, when the I-G is reviewing files and he comes across material relating to that, he has a duty to bring it to the attention of the defence team, which seems to me a much better method. I am not challenging your ultimate problem here, but there are a lot of little bits and pieces. You are saying, ‘They can tap phones in Australia.’ They do not, they cannot.

**Mr O’Gorman**—But they can.

**Senator ROBERT RAY**—This does not override the telephone intercept act. It does not.

**Mr LEO McLEAY**—Are you satisfied with the way ASIO acquires material in Australia?

**Mr O’Gorman**—How can I answer that question, with respect?

**Mr LEO McLEAY**—If you as a lawyer were satisfied with the way ASIO acquires telephone taps to get information and ASIS acquired information within Australia in exactly the same way, would your fears be allayed?

**Mr O’Gorman**—No, because my concerns are just as applicable to ASIO, but I did not come here to talk about ASIO. To answer your question: the same concerns apply because section 11 moves the functions of ASIS beyond what are regarded as your traditional spook, national security functions. It talks about ‘national economic wellbeing’. What does that mean? If there was, to use the Cybercrime Bill aspect of this inquiry, a large scale computer attack on an Australian commercial entity—and, as I see it, economic wellbeing is not defined, so it may well encompass that—and someone is then criminally charged arising from that, and if ASIS has been involved in gathering information because it fits within ‘economic wellbeing’, my concerns about having a machinery to say to IGIS, ‘Can you check to make sure that there is nothing there that might be relevant to the defence’, still exist. I repeat: section 11 terms are not defined, particularly the concept of what economic wellbeing means.

**Mr MELHAM**—Can I then summarise: a lot of your concerns have to do with clarity of language in terms of this bill and also the fact that it could be more precise in terms of definition. There is a lack of definition.

**Mr O’Gorman**—Yes. There is a lack of definition, but I would go further and say that there has to be this machinery for access to IGIS in individual court cases. But, yes, what does economic wellbeing mean? What does foreign relations mean? National security, as I understand the cases, is pretty well defined, but I am not aware that the cases have defined the concept of ‘economic wellbeing’. What does that mean?

**Mr MELHAM**—Do you believe the definition of police functions should be in there?

**Mr O’Gorman**—Police functions definitions should be certainly in the definitions section.

**Mr BRERETON**—In your submission, you made reference to the New Zealand provision which specifically prevents their agency from spying on a New Zealand citizen. Would you like to elaborate on that?

**Mr O’Gorman**—That is on page 8.

**Mr BRERETON**—And then it is again on page 9.

**Mr O’Gorman**—I firstly refer on page 8 to the article in the *Sun-Herald* of 1 July, which said:

While the new bill is supposed to protect the privacy of Australian citizens, this can be overridden by other provisions. Unlike the safeguards contained in New Zealand intelligence laws, members of Australian non-government organisations could be targeted by ASIS and DSD if their activities were felt to be harming relations with another country.

A future Malaysian or Indonesian government, for example, could complain about an Australian non-government organisation (NGO) campaigning against the logging of rainforests in Borneo. ASIS and DSD could then monitor the NGO’s phones. The NGO’s computers could be hacked into...

I am not aware that anyone is saying that the author of that article in the *Sun-Herald* is wrong. I have included it to indicate that, if a smaller country like New Zealand can contain safeguards to protect their citizens from being targeted by the intelligence agencies, at least with respect this committee should consider it.

I am aware that probably my time is close to being up. Can I refer to the concerns about cryptography on page 10?

**CHAIR**—I was just going to move on to that if we could.

**Mr O’Gorman**—Section 7(d) provides that the DSD can provide assistance to Commonwealth and state authorities in relation to cryptography and communications technologies. The issue of cryptography has been an extremely controversial one, both in the United States and in the UK in the last two years or so. I then refer to an article from the American Civil Liberties Union webpage, which says:

Cryptography provides an envelope, seal and signature for otherwise unprotected electronic communications, including telephone conversations, fax messages, e-mail, fund transfers, trade secrets and health records. Without strong encryption, there will be no way to protect private communications from snooping, whether by the government, by business competitors, by terrorists, or by nosy neighbours, hackers and thieves. The ACLU therefore supports the free and unfettered development, production and use—

not by law enforcement agencies, but by citizens—

of the strongest possible encryption technology.

The last indented paragraph on page 11 continues that quote:

Today’s debate over cryptography offers the nation an opportunity to confront the issue of electronic surveillance anew. The ACLU believes that electronic surveillance is absolutely inconsistent with a free society. Free citizens must have the ability to conduct instantaneous, direct, spontaneous and private communication using whatever technology is available. Without the assurance that private communications are, indeed, private, habits based upon fear and insecurity will gradually replace habits of freedom.

The only point of putting that in is to say that in section 7(d) lurks, in my view, a real problem. I will abstain from more strong language, but where is section 7(d) going to lead where it says:

The DSD can provide assistance to Commonwealth and state authorities—

for that read ‘domestic law enforcement agencies’—

in relation to cryptography.

It is a huge debate in the United States where, under President Clinton, it was in fact an offence in some areas for citizens to have encryption material on their electronic communications that domestic law enforcement agencies could not crack. If we are going to have that debate in Australia, my contention is: let us not have that development buried in section 7(d). I have a very real concern about what section 7(d) means.

**Mr ANDREWS**—But this is not being suggested by this legislation, is it?

**Mr O’Gorman**—What does section 7(d) mean, if I might ask rhetorically?

**Mr ANDREWS**—Doesn’t it simply mean that law enforcement agencies, with the assistance of the DSD, can actually try to keep up with those who might wish to encrypt material for the purposes of endangering the national security of Australia? Taking the American Civil Liberties Union’s argument to its logical conclusion, we might as well give up on any sense of an intelligence service and, for that matter, we might as well give up on trying to keep up with anybody who would want to encrypt material which could ultimately be used adversely against Australia.

**Mr O’Gorman**—No. With respect, I am not going that far; I am simply saying that this raises, for the first time that I have seen in any federal legislation, the issue of cryptography.

**Mr ANDREWS**—There is nothing in this, as I read it, that says that a citizen or a company or any other entity in Australia cannot engage in encryption procedures. It simply says that the DSD can assist—to use your language—law enforcement agencies in relation to cryptography and communications technologies. I would have thought that we would want to do that.

**Senator ROBERT RAY**—It is very broad. I can give you one example: if I wanted to communicate with the Victorian Agent-General in London by e-mail it would go via DSD, because they provide the encryption for the information to go and come back. And I assume they do that for a lot of diplomatic and other issues. That is why I think the Commonwealth and state authorities are in there. We probably disagree philosophically on what we should decrypt and what we should encrypt but I do not think we should have that argument here today, because we are just not going to agree.

**Mr O’Gorman**—I did not come here today expecting people to agree with me, necessarily.

**Senator ROBERT RAY**—I understand that.

**Mr O’Gorman**—The Commonwealth authority is defined in the definitions section as an agency within the meaning of the Public Service Act; it does not just mean secret national security.

**Senator ROBERT RAY**—I agree.

**Mr O’Gorman**—I am not seeking to overstate what I am saying about cryptography. I am simply seeking to draw attention to the fact that a secretive organisation called DSD can provide cryptographic technical assistance to federal and state authorities. I am simply asking, not this committee but rhetorically, whether the whole debate about cryptography has to be much more public.

**Senator ROBERT RAY**—I do not know if I agree with that.

**Mr MELHAM**—When you say public, I assume that what you are also saying is that there has to be some limitation on this. From your point of view, the way the bill currently is—and I think this is where you pick up the American Civil Liberties Union—you are concerned that we will enter into a new era in relation to surveillance if this were to go through the way it is, without public debate or without public scrutiny.

**Mr O’Gorman**—Mr Melham, you have put it better than I was able to. I am concerned. If a secretive organisation called DSD is to provide cryptographic technology advice to very widely defined federal and state government authorities, we should have a debate about it rather than have it buried in section 7 (d). Let us have a debate about what is happening with cryptographic technology and what law enforcement agencies in this country may be able to do with that in due course to interfere with citizens’ private communications. And I stress, ‘in due course’.

**Senator ROBERT RAY**—It is not actually being sneaked in at all. Putting DSD under a legislative base is probably recognising things that it has done in the past. Yes, it is in legislation for the first time but it is not being sneaked in. It is recognising the gamut of things that DSD has been involved in over last years.

**Mr O’Gorman**—Perhaps I should have said that it is buried there and that you have to dig for it to notice it.

**Senator ROBERT RAY**—We agree that it is not very well defined but I do not think that it has been snuck in, or even buried.

**Mr MELHAM**—Do you say that if DSD has a legislative base, a legislative recognition, which it is now getting for the first time, that you are concerned about how this is actually going to be implemented or—

**Mr O’Gorman**—Used in due course down the line, yes.

**Mr MELHAM**—There are not even limitations such as reasonable suspicion or a whole range of other others?

**Mr O’Gorman**—All those issues are not addressed.

**Mr MELHAM**—From your point of view, the way this is dealt with needs to be looked at a lot more carefully and closely.

**Mr O’Gorman**—The issue of a highly secretive agency such as DSD being able to provide cryptographic technical assistance to domestic law enforcement agencies is one that needs much greater exposure and debate.

**Mr MELHAM**—As it currently stands, it is unfettered and unqualified, isn’t it?

**Mr O’Gorman**—As I read it, it is. I agree that it does not go as far as suggested by one of the other committee members and that, by itself, it permits state or federal law enforcement agencies without further legislation to engage in decoding of the encryption. I am simply saying that it is a debate we should have, and it is something, I suppose, that I am trying to put on the table.

**Mr LEO McLEAY**—Can you give me some idea about why you think that police and Commonwealth agencies being able to make more secure their communications is such an important issue?

**Mr O’Gorman**—No. With respect, that is not what I am saying. DSD will be able to give cryptographic advice as to how state and federal law enforcement agencies can interfere with your and my electronic communications in due course.

**Senator ROBERT RAY**—It is a two-way street.

**Mr O’Gorman**—Indeed, I acknowledge that for national security reasons—I have greater doubts about economic wellbeing reasons—communications by DSD, ASIO and ASIS should be cryptographically intact. I am looking at it from the other way round.

**Mr LEO McLEAY**—I missed that point; I am sorry.

**CHAIR**—Let us move on to the last section.

**Mr O’Gorman**—The last section has to do with ministerial guidelines on privacy.

**Mr MELHAM**—You mention ministerials on page 10 of your submission, don’t you?

**Mr O’Gorman**—No. My concern is that the committee is prohibited, as I read it, from even examining the privacy guidelines that the minister lays down.

**Mr MELHAM**—There is something on ministerial direction on page 7.

**Mr LEO McLEAY**—At the bottom of page 9, your submission refers to the weakness of the committee’s supervisory role being reflected in section 7 (d).

**Mr O’Gorman**—Yes, thank you. I simply want to bring your attention to this point in my submission:

The weakness of the Committee’s supervisory role is reflected in Section 29 (3) (f), which indicates the functions of the Committee do not include reviewing the privacy rules made by the Minister regulating the communication and retention by ASIS or DSD of information concerning Australian citizens.

My submission is that, if the committee cannot even do that—

**Senator ROBERT RAY**—I agree with that, but the committee can do it indirectly because one of the people it can call to cross-examine on this is the Inspector-General. So the committee can do it indirectly but not directly.

**Mr O’Gorman**—My submission is that the committee should be able to do it directly.

**CHAIR**—Thank you, Mr O’Gorman.

**Mr MELHAM**—Mr O’Gorman, I believe you are going to be here tomorrow.

**Mr O’Gorman**—Yes. I will stay around tomorrow to hear the submissions of the other witnesses.

**Mr MELHAM**—I notice that you want an opportunity to make a supplementary submission to the committee. Mr Chairman, I am just wondering, if there is time, whether we might circumvent that tomorrow by Mr O’Gorman commenting on some of the evidence that we receive, if he wants to.

**CHAIR**—I think that is a good idea, because we are probably not going to have the roundtable after the hearing.

**Mr MELHAM**—Mr O’Gorman, are you happy to be given that opportunity to comment on evidence that we might receive from other witnesses tomorrow, if we have the time?

**Mr O’Gorman**—Yes.

**CHAIR**—Thank you, Mr O’Gorman. We will send you a copy of the transcript and the secretary will be in touch if we need any more information.

[4.15 p.m.]

**BLICK, Mr William James, Inspector-General of Intelligence and Security, Office of the Inspector-General of Intelligence and Security**

**CHAIR**—Although this committee does not require you to give evidence under oath, I should advise you that these hearings are legal proceedings of the parliament and warrant the same respect as proceedings of the House or the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Do you wish to make some introductory remarks before we proceed to questions?

**Mr Blick**— I do not think so, Mr Chairman.

**Senator ROBERT RAY**—Whilst you have no introductory remarks, I think a recurrent theme of concern has been about the immunities issues and the way ASIS deals with Australian citizens. I think you might be able to clarify that up front, before we get into detailed questions.

**Mr Blick**—I guess I should approach it from the point of view of the operations of my office, fundamentally. As far as the immunity provisions are concerned, certainly in the last year or two—and probably before that—I have observed instances when the two agencies under consideration have needed to look very carefully at the legality of operations they were proposing to become engaged in. I have certainly come across instances where the legal regime we have in Australia as it relates to, potentially, activities overseas has caused them to think very carefully about, and in some cases to obtain legal advice about, the operations that they wish to conduct, where those operations, in my view as the Inspector-General, should cause no difficulty for us as Australians and for the agencies concerned.

As I understand it, the intention of the legislation as it is drafted in that area is not to give open slather to members of the agencies to break Australian law; it is simply to provide them with targeted immunity in cases where the operation of Australian law is such that it may cause difficulties for those kinds of operations. I do not see any difficulty with that, given that my own office will, on a regular basis, be doing what it does: inspecting the operations of the agencies and ensuring that the capacity for the agencies to undertake these sorts of operations with that kind of immunity is not abused. I think it is fair to say that I have seen no instances of a desire on the part of the agencies to abuse their privileges in the past, and I have every reason to believe that they will not do so in the future. If I observed any instances of that, obviously I would take necessary action.

The second issue relates to privacy of Australians. A set of rules for each of the agencies is already in existence, and my office has been responsible for supervising the operation of that for a number of years. The rules that would be made under this legislation would be basically the same as the rules that are already in existence. I think there is scope for some tidying up and improvement of the rules because, inevitably with these kinds of things, you come across circumstances that mean that you need to make adjustments to them as time goes on. But I think that the rules are fundamentally sound and having them regulated by virtue of this legislation I think would be a good thing. The regime that the legislation provides for privacy is a robust

one. I believe too that having it regulated in the way that it will be regulated provides further insurance against abuse of the privacy rights of Australians.

**Mr LEO McLEAY**—I have a couple of questions arising out of Mr O’Gorman’s evidence. Mr O’Gorman indicated that he felt that ASIS was in a position to tap telephones in Australia. Are there circumstances where that can occur and, if it does, how is that regulated?

**Mr Blick**—The fact is that the telephone tapping regime in Australia is already highly regulated. In the national security area, the responsibility for telephone interception lies with ASIO and pursuant to warrants approved by the Attorney-General. I took Mr O’Gorman’s comments, if I may say so, with respect, as really being more of a concern about the interception regime in toto, rather than specific to ASIS.

**Mr LEO McLEAY**—I was going to come to that next. But your understanding is that ASIS themselves do not and are not able to tap telephones in Australia?

**Mr Blick**—That is precisely the case, yes.

**Mr LEO McLEAY**—What about Mr O’Gorman’s suggestion that, if ASIS comes across an Australian target and passes that information on to somebody else and that becomes the basis of the beginning of a prosecution, there should be some way of discovering that ASIS was the beginning of that evidence train? Do you have a comment on that?

**Mr Blick**—I think that could be encompassed within the current regime, not quite using the mechanics that Mr O’Gorman suggests. There are two things here. If ASIS, or DSD for that matter, became aware of information that they then passed on to Australian law enforcement authorities and down the track there was a prosecution, first of all, as more than one of you have said, there needs to be admissible evidence for the prosecution to be launched, and that needs obviously to arise from things other than provided by the intelligence and security agencies.

But let us suppose that we reach the hypothetical situation advanced by Mr O’Gorman—namely, that there is material revealed in intelligence collected by one of the agencies that could be suggestive that the individual concerned is not guilty of the crime of which they have been accused. My view would be that, if there were such material, it would be the duty of the organisation concerned to pass it on to the people responsible for law enforcement, and I would regard it as an issue of propriety within the terms of my legislation to ensure that that happened, provided that the information was significant. So from one point of view, there is already a mechanism whereby one can ensure that the agencies do not breach what I would regard as a responsibility that they should properly undertake.

Looking at it from the point of view of the people who are affected by this, the people who are going to be prosecuted, while there is not a legislative provision for what Mr O’Gorman refers to as subpoena, there are certainly provisions under the Inspector-General of Intelligence and Security Act enabling a person to lodge a complaint with the Inspector-General about the actions of the agencies concerned—that is, the various agencies within the Australian intelligence community, of which ASIS and DSD are two. So if a representative of a person who was being prosecuted wished to do so, they could certainly complain to me about their belief that an agency had not passed on information which might be exculpatory.

**Mr BRERETON**—I want to get an idea of how much time you put into supervising these two agencies under consideration at the moment. If you had to look at it on an average monthly basis, how much time do you find yourself spending on the ASIS case and the DSD case?

**Mr Blick**—It is a bit hard to put hours on it, but if you take the three agencies that have the most impact on the lives of people—ASIO, DSD and ASIS—my guess would be that probably 50 per cent of my inspection work would be to do with ASIO, and DSD and ASIS would have 25 per cent each, if I can put it that way. With DSD, we visit their premises roughly on a monthly or six-weekly basis and spend an hour or two going through the material that relates to the privacy of Australians—the operation of the rules. Also, quite frequently, either DSD will brief me on an operation that they are proposing to conduct and seek my advice on issues related to propriety or I will seek briefings on the progress of operations.

Pretty much the same applies with ASIS, except that ASIS would probably tend to brief me on different kinds of issues by and large from the ones that DSD would. I get more briefings from ASIS on things related to their personnel in the organisation, for obvious reasons, because their personnel are dealing with people overseas. But roughly I would say I spend an equal amount of time looking at their files. In fact, on reflection I would spend more time with ASIS, because we have a project to read every live operational file within ASIS over the next few years. That takes a great deal of time, and there are basically two of us doing that. So on reflection, I spend probably more time with ASIS than with DSD, where we are talking about electronic records by and large.

**Mr BRERETON**—So a couple of hours a month in one case over there plus the extras, and then a bit more than that with ASIS.

**Mr Blick**—Yes, quite a lot more with ASIS now I think about it, because we tend to go over and spend a day or two at a time reading through their files.

**Mr BRERETON**—So would it be a day a month?

**Mr Blick**—At least that.

**Mr MELHAM**—Is that limitation because of resource limitations on your part? Or do you find that that is all you require?

**Mr Blick**—With DSD, unquestionably the second is the case. You would be wasting your resources if you spent more time going through the material. With ASIS, it does relate to resources but on the other hand I do not regard it as a frantically urgent task either. It is something that I think ought to be fitted into a regular inspection regime. We also of course inspect the records of ASIS in relation to the nationality rules, the privacy rules, and that is a separate exercise from these regular file inspections.

As we speak, I am thinking of other things in relation to this. We also have online access to ASIS reporting in our office. I have an officer who spends some time every day going through all the ASIS reporting and the DSD reporting that is online to ensure that it complies with the rules that we have been speaking about. If I think of anything else as we go on, I will mention that as well.

**Mr LEO McLEAY**—To do your job, you are obviously familiar with the directions that the Minister for Foreign Affairs has given ASIS under the current regime and the Minister for Defence has given DSD. Are there any differences in those instructions to what is in section 6 and section 7 of this legislation?

**Mr Blick**—Do you mean: has this left anything out?

**Mr LEO McLEAY**—Have they put anything in?

**Mr Blick**—What is in this legislation gives legislative effect to what is in the directions.

**Mr LEO McLEAY**—And I am asking you: is there anything that has been left out or put in? Do section 6 and section 7 directly mirror the directions or are there differences? If there are, maybe you could tell us about them.

**Mr Blick**—Without the other directions in front of me, I cannot tell you the extent to which they exactly quote the current directions. But there is nothing in the functions, as described in this, that is not currently covered by the government's directions and there is nothing—

**Mr MELHAM**—Including 7(d) 'cryptography'?

**Mr Blick**—I would have to check that. You would probably need to ask DSD—

**Mr LEO McLEAY**—Could you come back to the committee with some advice about whether they mirror each other or whether there are changes?

**Mr Blick**—By all means, yes.

**Mr LEO McLEAY**—The reason I ask that is that we are being told that this puts on a legislative footing what is already happening. I would like to be quite sure that that is what we are doing.

**Mr Blick**—And you want me to tell you?

**Mr MELHAM**—Mr O'Gorman expressed some concern about lack of definitions—for instance, in terms of police functions and national security—in the legislation. Do you see your supervisory role as basically filling in that gap?

**Mr Blick**—Yes. I think the best answer is that, if you observe an activity that does not fit within these terms or if I observed an activity that, in my belief, did not fit within these terms, I would obviously want to be advised about whether the agency believed it did in fact fit within—

**Mr MELHAM**—Do you have guidelines in terms of what you regard to be police functions and what you regard to be genuinely national security matters?

**Mr Blick**—No, I do not, and I do not think I need them. In relation to national security, there is in fact a definition of ‘security’ in the ASIO Act, as I am sure you know. That provides, I think, a pretty reasonable working definition. Police functions have not been an issue in my experience because the agencies have never shown the slightest inclination to become involved in functions of that kind. My belief about this legislation is that the intention—and the minister may have a better view of this than I—is to spell this out so that it is clear on the public record, rather than to prevent the agencies doing something that they desperately want to do. It is quite clear to me that there is no intention on their part to do that, and they see their role and the police role as being fundamentally different.

**CHAIR**—On that line, are you perfectly happy that the new provisions in these bills are adequate to allow you to operate the way you would like to operate? Or do you think that there are some points that need to be reviewed or strengthened to ensure that you can do the job properly?

**Mr Blick**—I think the combination of these bills and my own legislation provides a very strong basis for doing the work that I have to do.

**Senator ROBERT RAY**—The crunch for most of us is: all right, there are limited immunities put in there that may be invoked, given a police prosecution or reference to the DPP—and I think we are gradually understanding what the processes are—but the question arises where that is not discovered by a state or federal enforcement body. If an illegal act occurs and is never tested as to whether it is relevant, what position are you in to make an assessment on that and report it to the relevant authorities if the illegal act is outside what was expected amid preparation for an overseas operation?

**Mr LEO McLEAY**—Or should you even be looking for that?

**Mr Blick**—Part of my functions under the Inspector-General of Intelligence and Security Act is to ensure the legality and propriety of the agency’s operations. So it is certainly within my function to do that. I suppose the best answer I can give to you, Senator Ray, is that, as I have mentioned before, in the course of our work we are inspecting every current operation of ASIS. If there were activities going on in the course of those operations that were illegal or improper, I would have the power to act upon that knowledge.

**Senator ROBERT RAY**—That is good. Are you satisfied you can make the interpretive decision? This allows, in very limited circumstances, illegal acts by those officers to be legal. Are you able to measure off the misdemeanour of the officer compared with what he is instructed to do in terms of what his or her role is?

**Mr Blick**—Yes, I think so. As you know, this provides a code in which the minister has to authorise activities. The authorisations will be very clear about the limitations on those activities, and I will have access to both the authorisations and the records of the activities. It would be very difficult for someone to breach their duty in a way that I would be unable to monitor.

**Senator ROBERT RAY**—Let us take a theoretical circumstance. There is no pursuit by the ACT police or anyone else, but you discover an illegal act has occurred and you do not think it is strictly related to the preparation. What steps do you take from that point on?

**Mr Blick**—The first step I would take would be to not trust my own judgment but to go and get some legal advice from adequately cleared and qualified people in the Australian Government Solicitor's Office. Then, depending on the nature of the illegal act I would, as I have previously agreed with the heads of the agencies, bring it to their attention and seek their response as to what they were going to do about it. Again as I have agreed with the heads of the agencies in formal letters, if they did not take action that was, in my view, adequate and appropriate in those circumstances, I would bring it to the attention of the minister. If that did not result in appropriate action, I would bring it to the attention of the Prime Minister. If the Prime Minister refused to act on it, I would have to think about it.

**Senator ROBERT RAY**—You do not have anything in your powers to go anywhere else, do you? You cannot report to parliament, can you?

**Mr Blick**—I can certainly report to parliament publicly, but there are limitations to that of a national security nature. I could certainly report to parliament if I believed that I had been up this chain—if I could put it that way—and that inadequate action had been taken as a result of what I had done. I would not need to specify the issue necessarily in order to do that.

**Mr MELHAM**—Was your office consulted on this legislation before it was tabled in the parliament?

**Mr Blick**—It certainly was.

**Senator ROBERT RAY**—Could I ask a minor question, in that case? It is noted somewhere that DIGO, having been so recently formed, does not come within your ambit. But there is an agreement that, for the purpose of the way they behave, it is taken as though they do. Why in heaven's name wasn't a suggestion made that this be slipped into this consequential bill so that they would be brought within your ambit under schedule 2? With all these minor clean-ups, why wasn't this one added in here?

**Mr Blick**—It has been a matter of timing.

**Senator ROBERT RAY**—I could draw up an amendment in five minutes and move it in the Senate.

**Mr Blick**—But, as I understand it, there are quite a number of pieces of legislation that affect the operations of DIGO. It is not just a matter of my legislation, it is also a matter of things like the freedom of information legislation and so on. I have been in discussions with the various agencies about this, and in due course—I do not think it will be very much longer—there will be legislation brought forward.

**Senator ROBERT RAY**—Fair enough.

**Mr LEO McLEAY**—One of the things that this legislation does is to set up a committee on ASIO and ASIS. One of the points that has been exercising our minds is: why isn't it a committee on ASIO, ASIS and DSD? From where you sit, do you see any reason why DSD should not be brought within the purview of that committee?

**Mr Blick**—I am not sure that I am the appropriate person to comment on that. I think it is really a matter of policy for the government. From my point of view this legislation improves my capacity to do my job, but I do not think I can comment really on the ambit of the committees.

**Senator ROBERT RAY**—No, I do not think you can do that. Have you heard a persuasive argument advanced anywhere, however, that DSD should not be within the purview of the committee? It is a slightly different question.

**Mr Blick**—If I turn up tomorrow, I might hear one from the ASIS and DSD representatives.

**Senator ROBERT RAY**—We have not had one amongst the written ones so far.

**Mr MELHAM**—Did you just say, Mr Blick, that this legislation improves your ability to do your job?

**Mr Blick**—Yes, I think it does because it provides for various reports to be provided to me in relation to the various elements of this bill. I would not want to make too much of that. I have got pretty significant powers already and from my point of view this is really clarifying that I can have access to information that I would be expecting to get access to in due course anyway. But certainly I think that the various provisions that relate to my office in this are good provisions and represent an improvement.

**Mr MELHAM**—In discussions in preparation for tabling this bill, were your concerns all met?

**Mr Blick**—Absolutely, yes. I do not want to get this out of perspective. I do not have any major concerns. This was really a matter of ensuring that it is absolutely clear that the operations of these agencies are not just subject to my scrutiny by virtue of my legislation but that there are particular things provided for in this legislation where my office has to be involved. For example, the minister is required to consult with me about the rules that are made to protect the privacy of Australians. That was not a provision in the existing legislation but it is a provision in this one.

**Mr MELHAM**—But what does 'consult' mean? It does not require your approval.

**Mr Blick**—It does not require my approval. De facto, what it will mean, as with the previous set of rules, is that I am involved in the drafting of the rules with the agencies concerned and that by the time the minister gets to sign off on them I will be happy with them.

**CHAIR**—How do you fit in with ministerial directives and the issuing of various authorisations? Do you get a say in that in these sections with ASIS?

**Mr Blick**—The current situation, which is basically continued by this legislation, is that the directives to the agencies—the overarching directives, if I can put it that way—are decided by the government but have to be provided to me. That is continued by this legislation and there is no formal requirement for consultation with me by the government in drafting those directives. I do not think there is any particular need for there to be, unless there were an issue about propriety in relation to a directive, when I would expect that probably the government would consult me.

With regard to authorisations, the authorisations are for particular activities and there is a requirement under this legislation that they be available for my perusal. As I think I have explained, it is generally the case that major operations that, as it were, break new ground would be matters that the agencies would at least speak to me about or brief me on, and perhaps on occasions consult me about if there were issues of legality and propriety. So, to answer your question, that is roughly where I fit into the thing.

The other thing I did not mention before when I was talking about our inspection activities is that, both in relation to DSD and ASIS, I annually inspect all the submissions that these organisations put to their minister. They keep sets of them and I go over once a year and look through all those ministerial submissions. Again, that is a matter of satisfying myself that the minister has had adequate information about the individual operations of the agencies.

**CHAIR**—There being no further questions, I thank you very much indeed, Mr Blick, for being with us today and for the forthright way in which you answered our questions. We will send you a copy of the record of the hearing and the secretary will be in touch if we need more information.

Resolved (on motion by **Senator Ray**):

That this committee authorises publication, including publication on the parliamentary database, of the proof transcript of the evidence given before it at public hearing this day.

**Committee adjourned at 4.45 p.m.**