COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE ON AUSTRALIAN SECURITY INTELLIGENCE ORGANIZATION

Reference: Australian Security Intelligence Organisation Legislation Amendment Bill 1999

TUESDAY, 27 APRIL 1999

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**

JOINT COMMITTEE ON THE AUSTRALIAN SECURITY INTELLIGENCE ORGANIZATION

Tuesday, 27 April 1999

Members: Mr Jull *(Presiding Member)*, Senator Sandy Macdonald, Senator MacGibbon and Senator Ray and Mr Forrest, Mr McArthur and Mr McLeay

Senators and members in attendance: Senator Sandy Macdonald, Senator MacGibbon and Senator Ray and Mr Jull and Mr McArthur

Terms of reference for the inquiry:

Australian Security Intelligence Organisation Legislation Amendment Bill 1999

JOINT COMMITTEE ON THE AUSTRALIAN SECURITY INTELLIGENCE ORGANIZATION

Tuesday, 27 April 1999

Members: Mr Jull *(Presiding Member)*, Senator Sandy Macdonald, Senator MacGibbon and Senator Ray and Mr Forrest, Mr McArthur and Mr McLeay

Senators and members in attendance: Senator Sandy Macdonald, Senator MacGibbon and Senator Ray and Mr Jull and Mr McArthur

Terms of reference for the inquiry:

Australian Security Intelligence Organisation Legislation Amendment Bill 1999

WITNESSES

Committee met at 10.05 a.m.

BOWMAN, Mr Norman Allan, Acting Principal Legal Officer, Attorney-General's Department

REABURN, Mr Norman, Deputy Secretary, Attorney-General's Department

HALY, Ms Margaret, Assistant Commissioner, Law Design and Development, Australian Taxation Office

MULLIGAN, Mr Rory, Acting Assistant Commissioner, Internal Assurance, Australian Taxation Office

MONTANO, Ms Elizabeth Maria, Director, AUSTRAC

BRYAN, Mr Neville, Senior Investigator, Inspector-General of Intelligence and Security

McLEOD, Mr Ronald Neville, Acting Inspector-General of Intelligence and Security

RICHARDSON, Mr Dennis James, Director-General, ASIO

PRESIDING MEMBER—I declare this public hearing open and welcome you all to today's hearing of the parliamentary Joint Committee on the Australian Security Intelligence Organization. The hearings are part of the ASIO committee's review of the Australian Security Intelligence Organisation Legislation Amendment Bill 1999, which has been referred to the committee by the Attorney-General. The committee has been asked to review and report on the bill within a very short time frame. Our report, in fact, is due by Friday week—that is, by Friday, 7 May 1999.

A number of non-government organisations and private citizens with an interest in the subject matter of the bill have made the point to us that it is very difficult for them to make submissions to the committee within such a short time frame. We recognise these difficulties and acknowledge that there are some people who would have liked to have appeared before the committee today but who in the time available were unable to make arrangements to do so.

However, I think it is important to acknowledge also the significance of the fact that the parliament is conducting a public review of this legislation. It is a rare opportunity for public input into the legislation underpinning the operation of ASIO. It is also a sign that our intelligence community and our government have a mature understanding of accountability—more so than perhaps has been displayed in the past.

The hearing today will involve three sessions. The first will be a government officials' round table with the Director-General of Security, officials from the Attorney-General's Department, the Australian Taxation Office and the Australian Transaction Report Centre, and the Inspector-General of Intelligence and Security. The second session will feature evidence from Mr Chris Connolly from the Financial Services Consumer Policy Centre, and in the final session we will invite the lead government witnesses, the Director-General of Security and representatives from the Attorney-General's Department to appear again to wrap up any outstanding issues and comments on the evidence presented during the day.

I advise those present that the Attorney-General has agreed, in accordance with section 92F of the Australian Security Intelligence Organisation Act 1979, that these proceedings should be conducted in public session with two exceptions. The exceptions are that the Director-General of Security wished to give part of his evidence in camera and that issues may arise during questioning that government officials may ask to respond to in camera. In order to cause minimal disruption to our proceedings, I propose that in both cases the taking of evidence in camera be delayed until the final stages of the hearing, when the committee will move into private session.

I also advise those proposing to give evidence this morning that, although we will not be requiring you to give evidence under oath or affirmation, these hearings are legal proceedings of the parliament and warrant the same respect as proceedings of the House and the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament.

To begin the first session, I call the witnesses participating in the government officials' round table. I understand that the Director-General has some introductory remarks that he would like to make before we proceed to consider the bill in detail.

Mr Richardson—I will not go over the detail of the bill—firstly, because it is before you and, secondly, because there is the explanatory memorandum and also the second reading speech. However, by way of

introduction, there are some points worth making on the background to the proposed amendments and the major thrust of those amendments. The proposed amendments are the outcome of a review conducted by government against the background of ASIO's own experience and, more importantly, technological change over the past 20 years. I believe the committee is aware that the current act has been in operation since 1979, having been subject to only one round of major amendments in 1986. The purpose of the proposed amendments is six-fold.

The first purpose is to update ASIO's powers to enable the organisation to utilise 1990s technology in carrying out its functions as defined in the act. Examples of this are the proposed amendment relating to computer access, the proposed amendment relating to the use of tracking devices and the proposed amendment relating to the carriage of articles by private contractors.

The second purpose of the proposed amendments is to enable ASIO to access information which is essential to its investigations in the areas of tax and also financial transactions. Those amendments are part of the package you have before you but entail amendments, not so much to the ASIO Act, but to the taxation act and to the Financial Transactions Reports Act. Different people from other organisations can of course address any queries you have on that in more detail.

I make the following points in relation to that access. Firstly, on occasion, access to taxation information and to financial transactions can be critical in ASIO's work—especially in the area of counter espionage and also in the area of politically motivated violence or terrorism. Indeed, in respect of the latter, before the end of the year there is likely to be an international convention which will call for governments to be more aware of the need to access information relating to financial transactions in the fight against terrorism.

The second point I would like to make in this area is that the proposed amendments provide ASIO with no more access than the access which law enforcement authorities currently have. Indeed, the access ASIO would have under these amendments in respect of financial transactions would be less than the law enforcement authorities currently have. A third point is that access in respect of both tax and financial transaction information would be subject to an MOU and also—particularly in the case of financial transactions—subject to a monitoring role by the Inspector-General of Intelligence and Security.

The third purpose of the proposed amendments is in respect of one matter specifically relating to the Olympics next year, and the capacity of the organisation to pass information directly to state authorities in the process of security clearances and the like.

A fourth purpose of the proposed amendments is to make some changes to the warrant provisions, particularly to emergency warrants and to the period of validity for search- and-enter warrants. A fifth purpose of the proposed amendments is to correct some anomalies which we currently have to operate with. One is our inability outside a period of a warrant to remove listening devices which may have been put in place as a result of a warrant. Another example is our inability at the moment to collect foreign intelligence in Australia through the use of human sources. The final purpose of the proposed amendments can be put under the miscellaneous heading. Firstly, it goes to the issue of cost recovery. Secondly, it goes to the issue of the organisation's capacity to pass intelligence directly to the AFP which it may receive from its liaison partners overseas.

They are the specific purposes of the proposed amendments. I would make some general comments flowing from that. First of all, only one of the proposed amendments is Olympics specific. The timing of the introduction of the bill, however, is relevant to the Olympics. If there is a need for the powers to be updated, it clearly makes sense for that to be done now rather than later.

The second general comment I would make is that all the proposed changes are within the existing accountability arrangements within which ASIO operates. They are outlined in detail in the submission that has

been put before the committee by the Attorney-General's portfolio, but I might briefly summarise what those accountability arrangements are. First, there is a statutory definition in the ASIO Act of what the organisation's functions and special powers are. Secondly, there is ministerial direction. Thirdly, there is a tight system which surrounds the issuing of warrants for the exercise of ASIO's special powers.

I might go through the approval process for warrants. First of all, within ASIO any warrant proposal must be approved within the collection area by the head of that division. Secondly, it must be approved by the legal adviser. Thirdly, the request must be signed by the Director-General personally. It is not an authority which is delegated. Fourthly, any warrant request, after it is signed off by the Director-General of Security, goes to the Attorney-General's Department where a separate certificate is signed advising the Attorney that the warrant request is consistent with the act. Finally, warrant requests must be considered and approved by the Attorney-General personally. Again, they are not matters which the Attorney-General can delegate.

Beyond that, the Inspector-General of Intelligence and Security reviews all warrant files on a regular basis. Beyond the arrangements which relate to warrant approvals, and carrying on with the accountability arrangements which surround the organisation, there is a requirement in the act that there be regular consultation with the Leader of the Opposition in the House of Representatives. Secondly, there is a requirement that the Leader of the Opposition be furnished with a copy of ASIO's classified annual report. In other words, the same report that goes to government on an annual basis is also provided to the Leader of the Opposition. There is, of course, the joint parliamentary committee. There is also the individual right or the right which individuals have to seek an independent review of certain decisions taken by the organisation—for instance, in respect of security clearances.

In terms of the accountability arrangements which surround the organisation, part of the package of amendments which you have before you, Mr Chairman, is a package of three or four amendments relating to the act under which the Inspector-General of Intelligence and Security operates which makes his or her own power in some areas more explicit. But that is something which you might wish to pursue with the Inspector-General himself.

In summary, I believe the changes which are proposed are essential if ASIO is to remain effective, particularly in the context of technological change over the last 20 years. The other changes amount to a tidying up of some provisions which I believe are long overdue. The final point I would make is to go back to the accountability regime. I simply conclude by saying that all the proposed amendments are within the envelope of the very strict accountability machinery which properly surrounds the organisation.

PRESIDING MEMBER—Thank you, Mr Richardson. Just as a matter of background, could you tell us how long the legislation took to draft and who was consulted?

Mr Richardson—The proposed amendments were given early consideration as long as two years ago. It has involved consultation within the Attorney-General's Department, with each of the agencies represented along this table, with the Department of the Prime Minister and Cabinet, with the Department of Foreign Affairs and Trade, with the Treasury, with the Department of Defence and with other members of the Australian intelligence community not represented here this morning.

Senator ROBERT RAY—When is it hoped that the amendments will be in place?

Mr Richardson—As soon as possible.

Senator ROBERT RAY—Do you mean the powers of ASIO do not go so far as to understand the Senate process?

Mr Richardson—It is why the word `possible' is used.

Senator ROBERT RAY—But would Christmas do? Because that is what my guess is.

Mr Richardson—I do believe it is important from where I sit that those amendments which the parliament agrees to are in place before the end of the calendar year.

PRESIDING MEMBER—I am not quite sure how the committee would like to handle this, but I thought if we went through the schedules it might be a little more organised.

Senator ROBERT RAY—Does that give other witnesses a chance to intervene as we go if we do it schedule by schedule, not just ASIO at the one time?

PRESIDING MEMBER—Yes.

Senator ROBERT RAY—That would be good.

PRESIDING MEMBER—I would like to kick off with schedule 1. There is one point where the bill changes a definition. The definition of `permanent resident' becomes `unlawful non-citizen' or `illegal entrant'. Does that change the scope of the ASIO Act at all?

Mr Richardson—My understanding is that that proposed amendment is purely a definitional change flowing from changes to the Migration Act. In other words, it is merely ensuring that the definitions in our act are consistent with the definitions in the Migration Act.

PRESIDING MEMBER—The other thing that I picked up from the first section was schedule 2, section 14, which states:

The Bill proposes to allow the Minister rather than the Governor-General to appoint an acting Director-General.

Does this really reduce the transparency of the process and the number of levels of approval required in that process?

Mr Richardson—I stand to be corrected, but I think it does reduce the number of levels in the approval process. I do not believe it makes it less transparent, and I believe it is consistent with other changes that have been made to other legislation. I think it is merely trying to make the approval process in relation to acting directors-general quicker and smoother. However, the need for the Prime Minister to consult with the Leader of the Opposition in the House of Representatives is unaffected by the proposed amendment.

PRESIDING MEMBER—Another area of interest is the section regarding the charges of fees for services. What sorts of services will be charged for and by whom?

Mr Richardson—First of all, it would not relate to our core security intelligence advice. We currently have the power to charge other Commonwealth agencies for protective security advice. If this amendment were to be approved by the parliament, it would enable the organisation to charge non-Commonwealth agencies for the protective security advice that it currently provides.

PRESIDING MEMBER—And make a profit?

Mr Richardson—Not make a profit. It is cost recovery.

PRESIDING MEMBER—Would you ever have a situation where you are asked to perform a task like this and a particular person may not have the capacity to pay for it?

Mr Richardson—That is possible. I think there is provision in the proposed amendments which enables what may be charged to be varied. Indeed, there is provision in the proposed amendments for any fee to be waived.

PRESIDING MEMBER—I notice that it is the Director- General who can set that fee rather than the minister.

Mr Richardson—Yes.

PRESIDING MEMBER—What is the rationale behind that?

Mr Richardson—I believe the rationale is that it is an administrative, operational matter and therefore more appropriate for the Director-General rather than the Attorney-General.

Mr Reaburn—Mr Chairman, if you look at the amendment, you will note that the amendment does say that the amount of the fee must not exceed the reasonable costs to the organisation of giving the advice or providing the service. In that context, the Director General is the officer best suited to be able to make a determination of what is an appropriate fee.

Senator MacGIBBON—If you are saying you are not making a profit, this presupposes that you have a very accurate cost accounting base. Have you got a base that allows you to determine what it costs you to deliver a service?

Mr Richardson—Certainly.

Senator MacGIBBON—And it is accurate, is it?

Mr Richardson—I believe the extent to which it is less than accurate would be to the advantage of the user rather than the organisation.

Senator MacGIBBON—That was not my question, with the greatest respect. I asked you if you did have an accurate cost accounting basis.

Mr Richardson—Yes, we do.

Senator MacGIBBON—If you do, you would be the only department in the government that does.

Senator ROBERT RAY—I was about to suggest you might sell it to the department of finance.

Mr Richardson—I believe it is accurate—

Senator MacGIBBON—Go commercial with it.

Mr Richardson—in part because, in the protective security area, it is a fairly small part of the organisation and it is a discrete part. Therefore we can make its costings fairly accurate.

Senator MacGIBBON—You said that the bill proposes to allow the minister rather than the Governor-General to appoint the acting director-general and you said that was because of time constraints. How many times have you been embarrassed in the past by that time delay?

Mr Richardson—Personally, I am not aware of any, but I do not know whether that is the sole reason.

Senator ROBERT RAY—Is there any time limit? Is this an acting director-general while the then Director-General is away on leave or absent on other duty—

Mr Richardson—That is right.

Senator ROBERT RAY—or is it when the Director-General expires for some reason and you need an acting one before you can get the formal one? What exactly is it?

Mr Richardson—It is both.

Senator ROBERT RAY—Is that time limited?

Mr Richardson—Twelve months.

Mr Bowman—It is time limited to 12 months.

Senator ROBERT RAY—So, presumably, if you can appoint someone by the minister, you can also sack an acting director-general without reference to the Executive Council?

Mr Richardson—I do not believe so, but I am subject to correction on it.

Senator ROBERT RAY—What happens if you get an acting director-general you do not want or you discover they are not quite suitable or up to the task?

Mr Richardson—I believe an acting director-general could only be dismissed under the provisions relating to the dismissal of a director-general.

Senator ROBERT RAY—So it is a differential appointment but similar dismissal?

Mr Richardson—Yes.

Senator MacGIBBON—If you go back to paragraph 18(3)(c), this item repeals the paragraph and substitutes:

(b) where the organisation has come into the possession of the Organisation outside Australia or concerns matters outside Australia and the Director-General or the officer so authorised is satisfied that the national interest requires the communication—the information may be communicated . . .

to a series of people. If the information is so important that the Director-General is satisfied that the national interest is involved, why is the weak 'may' in there? Why not the information 'must' be transmitted? Why have you got the option?

Mr Richardson—It would depend upon the relevancy. We would get a lot of information that would be relevant within the organisation itself. There would be no need to pass it on to others.

Senator ROBERT RAY—There is a `may' there because on some occasions you would not pass the information on because it may compromise the source in the front line.

Mr Richardson—That is possible.

Senator ROBERT RAY—Is that why the `may' is there?

Mr Richardson—That would be another reason.

Senator MacGIBBON—But at the end of the day you would want to use the information?

Mr Richardson—Yes, certainly. Indeed, if there is such information and it is not passed on, then of course we are accountable for that and must stand to be judged accordingly.

Senator ROBERT RAY—And that has happened in the past, without going into any individual cases, hasn't it? You have had information you simply could not pass on because of the source.

Mr Richardson—Yes.

Senator ROBERT RAY—While Senator MacGibbon is looking for his next item: going back to the fee for service, if you like, that will be shown as an aggregate figure in your annual report?

Mr Richardson—Yes.

Senator ROBERT RAY—Just as an aggregate figure?

Mr Richardson—That is right, as it currently is.

Senator ROBERT RAY—Is this an area that you are going to encourage or discourage? It seems to me that, whilst it is valuable, it is not really your core business, is it?

Mr Richardson—No. We do have a responsibility under the legislation in the area of protective security advice.

Senator ROBERT RAY—Which implies it is a core function and therefore not chargeable in that sense. When you get pushed to the edges, I think it is absolutely appropriate to charge. Whether you do that is the appropriateness that I am asking about.

Mr Richardson—That is right.

PRESIDING MEMBER—I would like to move to item 16, which is the concealing of activities and the use of force. What monitoring mechanisms have you got in place to ensure that individual officers are only using necessary and reasonable force?

Mr Richardson—I suppose the general point I would make there is that, for what I think are probably self-evident reasons, we certainly would not have an interest, nor do I believe our responsibilities under the act would be served by us using any more force than is absolutely necessary. Clearly, for us to use any force beyond that would carry a real risk of what we are doing being in the public domain. So there is a very practical reason why we would not wish to use any more force than is necessary.

In terms of monitoring, again, the Inspector-General of Intelligence and Security has access to all our material, and it is open to any member of the public to make a complaint to the Inspector-General of Intelligence and Security about the organisation. Indeed, 18 or 20 complaints are made a year, so I think there is a mechanism whereby we certainly work on the assumption that were we to operate with any more force than is absolutely necessary, we would leave ourselves self-evidently open to investigation.

PRESIDING MEMBER—But you would not have any real definitions of what those limits might be?

Mr Richardson—Again, there are other people here who can give more of the detail, but I think you will find the formulation there is not inconsistent with the formulation in other acts. I think that formulation appears some multiple of times across different legislation.

Mr Reaburn—This is a provision that certainly the Attorney-General's Department would propose including in any warrant power for any organisation, and it is certainly the provision that appears in relation to law enforcement search warrants. Could I also make the point—and this emphasises the point that has already been made by Mr Richardson—that the kind of force that would be used by the organisation in executing a search warrant differs entirely from the kind of force that might be used by a law enforcement agency in executing a search warrant. When a law enforcement agency executes a search warrant, it has no concern about who knows that it has been done. Our organisation is more likely to find itself in quite a different circumstance. But any entry gained by the organisation would, within the realm of legal technicality, involve what the law calls force.

Senator MacGIBBON—Can I ask a general question about the security of ASIO's information? You would be aware that through the latter part of the last week the allegations were made that the Australian intelligence services had information about the actions of the militia and the ABRI in Indonesia in relation to Timor. With anything that appears in the Australian press, it is always very hard to know what is true and what is in the imagination of the journalist, but basically the claim was that there was a paper in hands other than government hands assessing the intelligence situation there. This has got rather profound implications for all the alliances we have with other agencies with which we exchange intelligence information, because if briefing papers end up in the hands of the press here quite obviously there will be a reluctance on other countries' parts. How good do you think your own retention of information is?

Mr Richardson—I think our own retention is excellent. I think there have been very few occasions in the last 20 to 25 years where there has been unauthorised information coming from ASIO. I think our own organisation has a very good record in that respect.

Senator MacGIBBON—You would agree here, though, that your access to information, particularly in a commercial area, is likely to be augmented by these amendments rather than decreased.

Mr Richardson—Sorry, I do not understand what you mean.

Senator MacGIBBON—The acquisition of information, particularly of a commercially sensitive nature, is likely to be increased rather than decreased by the amendments that are proposed in the new bill and therefore the need for you to maintain control of the information you hold to that extent is enhanced.

Mr Richardson—Certainly as a general proposition I would agree with that. I think, given the responsibilities of the organisation and given the information that it might have, both generally and also in respect of some individuals, there is a very big responsibility on the part of the organisation to ensure, firstly, that the only information it has is relevant to security as defined in the act; secondly, that it is properly protected

within the organisation and only people who have a need to know within the organisation have access to it; and, thirdly, that it is not released to the public unless that is authorised within government. I would agree with that.

Senator ROBERT RAY—The fact is that you no longer have another power to suppress that because D-notices are essentially dead and D-notices are essentially dead because organisations like the Australian Broadcasting Corporation will not comply, even though they are publicly funded. That is right, is it not? Brian Johns refuses to comply.

Mr Richardson—Yes.

Senator ROBERT RAY—All the newspaper editors agree to comply until they get their leak, and then they run it. So D-notices are dead; therefore it is your responsibility now. You are not backed up with that as your final defence.

Mr Richardson—Again, I would repeat that I think ASIO's record in protecting its information over the last 20 to 25 years is really excellent, and I would hope that it continues.

Senator MacGIBBON—I am not disputing that it has had a good record there but, like politics, every day is a new day and your past does not really count for much—it is the future that is important.

Mr Richardson—Put it this way: I have no reason to assume that our protection of information in the future will be any less rigorous than it is today.

Senator MacGIBBON—Let us move on to the changes proposed in section 16 on computer access. When did you first start breaking into computers?

Mr Richardson—We have not accessed computers using the technology that is currently available up until now because it would be illegal for us to do so—hence the purpose of these proposed amendments. However, we have been able to access information in computers through our search-and-enter warrants ever since we have had search-and-enter powers. Provided the warrant is properly drawn up, and provided the warrant provides the correct authorisation for search-and-enter then we have been able to access data in computers.

Senator MacGIBBON—This is presumably directed mainly towards the money trail rather than politically motivated violence or terrorist activities. It is unlikely that those people are corresponding by email or filing what they intend to do on computer files.

Mr Richardson—I do not think that is a fair assumption.

Senator ROBERT RAY—Emails, like faxes, are unbreakable, according to 90 per cent of the population—it is just a myth. In other words, people put things in emails that they would never put in a letter. Even in the returns to order we have had so far in the parliament you get better mining out of the emails than you do out of anything else.

PRESIDING MEMBER—In relation to that section, I would like to move on to the issue of extending the period of the warrants from seven to 28 days. We are also adding a potential commencement delay of another 28 days which, in actual fact, means that you have 56 days to do the business. Under the present conditions it is seven, so that is a massive expansion of that time. Why is it so necessary to increase those time frames?

Mr Richardson—Primarily because the current period of seven days is too narrow in the sense that

targets can vary their intentions and they can make last-minute decisions to do things differently from what we assessed. When that happens, we are required to go back, sometimes at very short notice, and get a second warrant. The proposed amendments are designed to add flexibility there in the activation of a warrant.

PRESIDING MEMBER—In terms of the computers, you have got the right to go in for six months. How does that stack up with provisions in other countries? Is that generally accepted as being the norm?

Mr Richardson—Yes, that is fairly consistent with what happens elsewhere. The proposed period of time for a warrant in relation to the computer accessing is the same as currently applies for listening devices and also telecommunications interception—that is, six months.

PRESIDING MEMBER—Do any of these amendments overrule any of the legislation that the states or territories might have? How do you get around that?

Mr Richardson—It would.

PRESIDING MEMBER—Were they consulted?

Mr Richardson—It does mean that, under the proposed amendments, with regard to obtaining access to data stored in a target's computer, provided we do that legally and properly under the warrant process, we would not be committing an offence under the Commonwealth Crimes Act or the equivalent state or territory laws. Again, that is consistent with our capacity at present to intercept telecommunications and our capacity to insert listening devices and the like; that is, provided we do that within the law, within the framework of the act. Again, that makes that action legal across the country.

PRESIDING MEMBER—I assume you consulted with the states and territories about that?

Mr Richardson—What is being done here is standard across the act. There has not been specific consultation with individual states and territories.

PRESIDING MEMBER—May I ask: if an individual finds that ASIO is accessing data on their computer, have they got any rights?

Mr Richardson—I would make two comments. First of all, if an individual did become aware of that then we have obviously failed in our professionalism. Secondly, if by some chance someone did become aware of that, then they would have the right to pursue that with the Inspector-General of Intelligence and Security. And, indeed, under the act we are not permitted to alter data and the like within the act, and if our actions were detrimental to the computer itself and its usage, I think people do have legal remedy against us.

PRESIDING MEMBER—If you get into a computer, are there safeguards that insist that ASIO would act appropriately in accessing that computer?

Mr Richardson—The same safeguards that exist with our use of listening devices and our use of telecommunications interception.

Senator MacGIBBON—You said that you have got the opportunity to intervene and plant a virus and rearrange a software program or something like that which you do not have with a listening device?

Mr Richardson—No, the proposed amendments would specifically make that illegal.

Senator MacGIBBON—Yes, but the opportunity is there, isn't it?

Mr Richardson—In theory, yes, but I would have thought that the organisation's own self-interest in terms of credibility, standing and acting lawfully would have some bearing there. We have accountability mechanisms both within the organisation and outside that I would have thought would minimise that sort of risk. Theoretically, telecommunications interception can be abused. Theoretically, listening devices can be abused. That is why—I think rightly—as an organisation we have very tight accountability arrangements put around us because, clearly, given the powers we have, there needs to be some additional accountability mechanisms put around us.

Senator SANDY MACDONALD—You said that if a listening device was discovered on a computer you would have failed in your professionalism. What is the nature of a listening device on a computer?

Mr Richardson—No, there would not be a listening device in a computer.

Senator SANDY MACDONALD—I was using that as a generic term.

Mr Richardson—The proposed amendments relate to remotely accessing data in a computer, so it is not actually necessarily about putting a device within a computer.

Senator SANDY MACDONALD—So that is accessing the information before it is encrypted?

Mr Richardson—Or maybe working your way through the encryption.

Senator ROBERT RAY—The relevant question in terms of interference with these computers is: are you entitled to interfere, to put a fault in the encryption equipment to make it withstand—

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

Senator SANDY MACDONALD—What about if the computer has mechanisms by which it protects its information?

Mr Richardson—That is a challenge for us.

Senator SANDY MACDONALD—You are not allowed to destroy or remove an alarm?

Mr Richardson—We would be allowed to compromise the protective mechanisms to an extent which would enable us then to access.

Senator SANDY MACDONALD—Is it technologically simple to bug a computer?

Mr Richardson—No, it is not simple. It can be very difficult.

Senator SANDY MACDONALD—Do you have a choice of where you can do it, before the encryption or in the encryption and in the computer itself?

Mr Richardson—Yes. If you were looking at accessing information in a computer, you would look at all

those options.

Senator ROBERT RAY—Coming back to your seven to 28 days for the warrants, I understand your core argument here is, unlike law enforcement agencies, you are doing this covertly, therefore the opportunity does not necessarily arise. Does this essentially, morally or ethically mean that you should attempt the insertion within seven days and only then use the rest of the time if it is not possible then—that it not be used as an excuse any time in the 28 days?

Mr Richardson—I think that is right, Senator. There is certainly an obligation on us, if the opportunity is there within those seven days, to do it within those seven days. Normally, that is operationally what you want to do anyway. When you go forward with a warrant request, particularly a search and enter one, you are doing it because the opportunity has arisen. Normally that opportunity is fairly narrow, so you have an operational interest in doing it sooner rather than later.

PRESIDING MEMBER—Perhaps we can move to the area of listening devices. Concerning the 28-day rule, how certain could we be about ASIO ensuring that the devices are deactivated when a warrant does expire?

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

PRESIDING MEMBER—So we can be assured that it is not a double-bunger effect; it really just gives you an opportunity to inspect premises twice under the one warrant?

Mr Richardson—No. Indeed, I think any operation that involves a physical entry—and normally putting in a listening device does involve a physical entry—is something that you want to do as few times as possible. The risk involved in going onto a property or entering a premise without others being aware is so high that it is not something that you play around with.

Mr McARTHUR—Could you give the committee a judgment on how many listening devices have remained on site because ASIO has been unable to remove them?

Mr Richardson—If it is possible, I would prefer to answer that question in camera.

PRESIDING MEMBER—That is fine. We have that provision.

Senator SANDY MACDONALD—I do not think it would be so confidential, would it? Under normal circumstances of a listening device being put in place, at the expiration of the warrant that would be removed as a matter of course, but it has to be within the time of the warrant.

Mr Richardson—That is right. At present, a listening device warrant is valid for six months and, if circumstances permit, the listening device is removed within that period. However, very often that is not possible.

Senator MacGIBBON—What happens when an ASIO officer enters a premise or organisation under a

bona fide warrant to acquire information and they are apprehended by the owner and taken before the courts for trespass? What happens then?

Mr Richardson—I do not know as it has not happened.

Senator MacGIBBON—Surely you should know, Director. Are you going to defend your officers or cast them loose?

Mr Richardson—Firstly, the operational planning is such that the chances of that happening are minimal—and I would be happy to take further questions on that in camera. Secondly, in the unlikely event that it did happen, our officers would obviously have an explanation for being there. In the unlikely event that it did happen and the owner wanted to take the matter further, then I assume they could, utilising whatever avenues they wished. At the same time, I would simply note that in such a situation our officers would have been on the premises legally. ASIO officers entering a premise under a lawful warrant are on the property lawfully. They are not on the property illegally.

Senator SANDY MACDONALD—Can they use necessary or reasonable force to search?

Mr Richardson—They would need to exercise some pretty good judgment with respect to that if they did not want to run into trouble with the law.

PRESIDING MEMBER—In conjunction with that, we will move on to the tracking devices. Is this provision just arranging for the extension of technological advancement or is it in fact a whole new area for ASIO to extend its powers?

Mr Richardson—I would see it in terms of modernising ASIO's power and enabling the organisation to utilise, as I said in my introductory remarks, 1990s technology. The organisation already engages in surveillance, quite obviously. It can do that without the use of its special powers. It does not require a warrant to put targets under surveillance. The technology is now available—it has been available for some years and is in use in many other countries—which enables an organisation such as our own to track objects through the placing of devices on the object. At the moment, there is nothing to prevent us utilising our own human resources to track an object. This enables us to do the same thing, but utilising available technology, and doing so more efficiently.

PRESIDING MEMBER—You have not had to have special legislation in the past for this. Have you had difficulties in the past?

Mr Richardson—No. My understanding is that the placing of a tracking device on an object without authorisation would constitute a breach of the law in terms of trespass. It would be trespassing, especially if it involved entry to property. Therefore, were we to place a tracking device on an object in order to follow it, we would need to have specific legal provision enabling us to do that; hence the proposed amendment. It is not done at present because we do not have the lawful authority to do it.

PRESIDING MEMBER—Would you have to maintain these devices for extended periods? If you did, wouldn't that be another excuse maybe to have multiple access to premises, vehicles or whatever you were using the device for?

Mr Richardson—The devices have a reasonable length of period of operation. They go for quite some months. However, I think the tracking device warrant is valid only for six months. So if we wanted to utilise it beyond six months, we would have to seek another warrant.

PRESIDING MEMBER—Item 24, section 27AA, gives you the opportunity to intercept the delivery of articles. I understand you have always had that ability with the post office. This will give you the facility to intercept objects from couriers, et cetera. Have you got the same powers in terms of your work with couriers and these other organisations as you have got with the postal services, or is that a bit different?

Mr Richardson—At the moment, our power to intercept and inspect postal articles is limited to those articles carried by Australia Post. Of course, that was fine in 1979. In 1999, it is ridiculous. Given the number of articles that are now carried by private deliverers and the like, our act in this area is really grossly out of date.

PRESIDING MEMBER—I would like to move on to item 33—that area of foreign intelligence—which says:

Item 33 extends ASIO's powers to collect foreign intelligence by means not requiring a separate warrant, on matters specified in a notice approved by the Minister.

How does this in fact expand ASIO's operational powers?

Mr Richardson—At the moment, we take the view on the basis of legal advice from the Attorney-General's Department, which I believe is correct—that is, our power is limited to what is authorised within the act. Within the act at present, ASIO is authorised to collect foreign intelligence within Australia through the use of its special powers. The act is silent on the question of ASIO's capacity to collect foreign intelligence in Australia outside the use of our special powers. Therefore, we take the view that that is not something we can do; therefore we do not do it.

Senator MacGIBBON—Would you explain precisely what you mean by that?

Mr Richardson—Under the current act we can collect foreign intelligence in Australia at the request of either the Minister for Foreign Affairs or the Minister for Defence utilising our special powers, that is, telecommunications interception, listening devices, and search and enter.

Senator MacGIBBON—The nub of it is that unless you are authorised you cannot collect foreign intelligence within Australia?

Mr Richardson—The nub of it is that we cannot collect it outside of the use of our special powers. The proposed amendments would give the organisation the lawful authority at the request of either the Minister for Foreign Affairs or the Minister for Defence to collect foreign intelligence in Australia through the use of human sources.

Senator MacGIBBON—So you are not getting any extra territorial power; you are not allowed to operate around Paris, New York or—

Mr Richardson—No, this is purely within Australia.

Senator MacGIBBON—That is not quite clear from the way it is written here.

PRESIDING MEMBER—I wondered about that because I thought you might have some sort of conflict with ASIS. I was going to ask how you manage that if there was.

Mr Richardson—No. First of all, it is territorially limited to within Australia. Secondly, it can be

activated only at the request of the Minister for Foreign Affairs or the Minister for Defence.

Senator MacGIBBON—How many liaison officers do you maintain in overseas posts at the present time—three or four, or more?

Mr Richardson—It is a small number. The precise number in location I would prefer to go to, if possible, in camera.

PRESIDING MEMBER—Is this arrangement similar to that given to other organisations overseas?

Mr Richardson—In what sense?

PRESIDING MEMBER—In terms of this section of your operation.

Mr Richardson—Yes.

PRESIDING MEMBER—Would that be reasonably comparable with—

Mr Richardson—Yes, very much so. Indeed, in most other countries, you would not require an amendment to legislation in order to do it.

PRESIDING MEMBER—Under this, with the extremes, could you, for example, utilise data collected at Pine Gap?

Mr Richardson—No, because we are not concerned with Pine Gap. That is not our responsibility.

Senator MacGIBBON—Let us come to the matter of oversight. You would be aware that the ASIO Act prohibits this committee from looking at any intelligence or any matter relating to a foreign national or to information derived from foreign sources or overseas. Why was that put in the act originally—presumably, it would have been at the request of ASIO?

Mr Richardson—I would not assume that it was at the request of ASIO.

Senator MacGIBBON—I would have thought that, when the act was amended in 1987 or 1986—whenever the last amendment was—there would have been extensive consultation between the government of the day and ASIO with respect to the setting up of the powers and responsibilities of the Joint ASIO Committee. There is a specific exclusion on matters in relation to foreign intelligence. I have never been able to determine why that exclusion was put in and what the rationale for it was.

Mr Richardson—If I can make two comments, the latter one of which will be guesswork on my part. The first comment is that, as you know, the amendments to the act in 1986 flowed from recommendations coming out of the second Hope royal commission.

The second comment I would make, which is more guesswork, is that it may be that it was considered inappropriate because we collect foreign intelligence in Australia not in our own right. We collect that on behalf of other agencies at the request of other ministers. It is possible that a view was taken at the time that the oversight of matters relating to foreign intelligence collection should properly reside in respect of those other areas of government that have responsibility for that. I do not know; I am guessing.

Mr Reaburn—That is the reason.

Senator MacGIBBON—In so far as one of the main stock-in-trades of ASIO is politically motivated violence and terrorist activities, with the situation in Yugoslavia and all the complexities of that and other events, surely the parliament has a legitimate claim to oversee the data collection methods that are so vital from a national security point of view or a community point of view.

Mr Richardson—I make no comment in respect of what oversight arrangements in relation to your own committee may or may not be appropriate.

Senator MacGIBBON—How are the powers of the Director-General exercised in relation to overseas intelligence by ASIO? Are those powers unfettered?

Mr Richardson—No, we do not—

Senator MacGIBBON—What oversight powers does the Inspector-General of Intelligence and Security have of your foreign intelligence activities? Are they complete and comprehensive?

Mr Richardson—For a start, the Acting Inspector-General can speak to that. I would make two points. First of all, we do not collect foreign intelligence outside of Australia. We do not have the lawful authority to do that; therefore, we do not do it. Our responsibilities in the area of foreign intelligence collection are defined within the act and they are limited to collection within Australia's borders. What we do do within Australia's borders in the area of foreign intelligence collection is done under warrant, and the same accountability processes which surround our other work also surround the warrants as such—that is, the Inspector-General of Intelligence and Security has access to our warrant files in that area.

The last point I might make, but which is really going into the Inspector-General's area, is that the Inspector-General of Intelligence and Security has, I believe, the same authority in respect of other agencies as what he has in respect of our own.

Senator MacGIBBON—Is the Acting Inspector-General satisfied that he has adequate oversight?

Mr McLeod—Yes. The comment that the Director-General just made is correct. The Inspector-General does have jurisdiction over both ASIS and ASIO, and the obligations of the Inspector-General in respect of those two organisations under the act are very similar. In particular, there is a concern on the part of the Inspector-General to ensure that the activities of both ASIS and ASIO, either separately or when they are working in cooperation with each other, are conducted lawfully and with a proper sense of propriety and in accordance with government guidelines. There is certainly no weakness in the accountability framework from the point of view of the Inspector-General being able to embrace the totality of the activity that we are talking about.

Senator MacGIBBON—Thank you.

PRESIDING MEMBER—Perhaps we can move on to the amendments concerning warrants. My understanding was that emergency warrants were usually issued for listening devices only. My understanding is now that virtually everything will be covered. Is it a regular occurrence that emergency warrants have to be issued? And what sorts of events might occur that would activate this requirement for the emergency warrants?

Mr Richardson—Just one comment by way of introduction. Under the proposed amendments emergency warrants would be extended to all warrants with the exception of those relating to foreign intelligence collection within Australia.

Since 1980, the Director-General of Security has signed three emergency warrants: once in 1981, once in 1986 and once in 1993. In terms of the individual circumstances, if you wished to go into that I would prefer to do that in camera, but I can make two generalisations. In each case, it has been a combination of, one, the short-term unavailability of the Attorney-General and, two, the assessed need for the warrant to come into force urgently and unexpectedly—that is, the need for a warrant to come into force within a matter of hours. They are the two conditions that have been met on each of the three occasions in the last 20 years when an emergency warrant has been required.

The other final points I might make are that, as you know, an emergency warrant approved by the Director-General is only valid for 48 hours and, secondly, it can be overturned by the Attorney-General short of that 48 hours. On each of the three occasions I mentioned, those first two conditions have been met; and on each occasion, as soon as the Attorney-General has become available, the warrant request has been put to the Attorney so that the Attorney had the opportunity either, one, to confirm it, to approve it, or, two, to overturn it.

PRESIDING MEMBER—Have any of them been rejected?

Mr Richardson—No, none of the three in the last 20 years.

Mr Reaburn—To clarify, at present the director has the authority to give emergency warrants in relation to both listening devices and telecommunications interception.

PRESIDING MEMBER—If there is nothing further on that section, perhaps we can move on to the Olympics, item 41. Could you tell us to what extent ASIO will be liable for the decisions and activities of the states and territories? To what extent would ASIO information on files be available to the states and, I suppose, to the Federal Police during the lead-up to and in the operation of the Olympics?

Mr Richardson—Essentially, the Olympics does not involve ASIO in a new area of activity. It essentially means that we have a lot more work to do within a compressed period of time. As you know, the responsibility for Olympic security resides with the New South Wales Police Commissioner, Peter Ryan. Our major role is, firstly, the provision of security intelligence and, secondly, the coordination of the federal government's intelligence input into the games.

We will have, as you know, a federal Olympic security intelligence centre within the ASIO building here in Canberra. That will seek to coordinate the collection and assessment by federal agencies of intelligence that might be relevant to the games. That will be passed on in the normal way to the New South Wales Police and/or to the AFP.

We will also have a role in respect of the games in terms of security clearances and accreditation, and that is where the proposed amendment comes in. At present, if a state authority wishes to receive a security clearance or security advice on individuals, it must do so through a sponsoring Commonwealth government agency—it is normally the Protective Security Coordination Centre in the Attorney-General's Department.

Because of the volume of work which we will be faced with in the lead-up to the Olympics—requiring 60,000 to 80,000 requests for security clearances within a very short period of time; and, despite everyone's best efforts, those requests will probably all come over the final three months or so—it would not be practical to utilise the existing system whereby each of those requests must go through a sponsoring Commonwealth agency and our response go back the same way. The proposed amendment seeks to cut out the middleman and it enables state authorities to come to ASIO directly and for ASIO to respond directly to the state authorities. That particular amendment has a sunset clause and would cease to have effect as of 31 December 2000.

Senator SANDY MACDONALD—Is a security assessment separate from information that is sought for a visa, or is it one and the same?

Mr Richardson—We will have requests in respect of, firstly, people entering the country and, secondly, people working in certain parts of the games. We will have to do security assessments in relation to both. The security assessments which I have been talking about relate not so much to overseas visitors, as there is a process there anyway, but more to people being accredited to work in different parts of the games.

Senator SANDY MACDONALD—And you will have 60,000 to 80,000 of those.

Mr Richardson—Yes, a minimum of 40,000 and a maximum of 80,000.

Senator SANDY MACDONALD—Can you do that in a legitimate fashion?

Mr Richardson—Yes. In the vast majority of cases it is a negative assessment rather than a positive assessment. In most cases the security assessment being made is whether an individual has a security record; it is not a full-scale individual assessment looking at the detail of background and the like. We would not be able to do that for 40,000 to 80,000 people over a three-month period.

Senator SANDY MACDONALD—You said that you had the existing power to deal with information concerning visa applicants. Do you expect to have a substantially increased number of requests in view of the number of people who are proposing to come to the games?

Mr Richardson—Yes, we will. Again, the challenge there will be the number of requests we are getting within a set time frame. It will be the fact that we are getting a large volume of requests over a two- to three-month period.

PRESIDING MEMBER—It makes Senator Ray's statement on the timing of the legislation even more critical.

Senator SANDY MACDONALD—That is right.

Senator ROBERT RAY—You have not seen the Senate timetable; if you had, you would be worried.

PRESIDING MEMBER—Just to finish off section 1, we have amendments relating to the review processes for former employees and current employees. Are these regulations which establish the review body available yet?

Mr Richardson—I understand that they are not. The answer to that is no.

PRESIDING MEMBER—Can you tell us why it is necessary to have this additional layer of appeal between ASIO and the Inspector-General?

Mr Strang—The first part of the proposal is to enable former staff who have a grievance which arose while they were on the staff to access the current grievance review mechanisms. At the moment, as soon as they leave the organisation all existing rights of review of grievances cease and the only avenue left is the Inspector-General. That is a perfectly good avenue, of course, but the Inspector-General himself in a case two or three years ago suggested it was better and more consistent with usual practice for the former officer to be able to go back to the internal grievance review body. That is the first amendment. The second is to give the

chairs and members of our disciplinary review committees the protections from civil actions for defamation and the like which are currently available to similar bodies set up under the Public Service Act.

PRESIDING MEMBER—Does that therefore give ASIO employees a greater appeal right in some respects than other members of the Australian Public Service?

Mr Strang—I cannot answer that question.

Mr Reaburn—We think not. We think the system is consistent with the kinds of grievance and grievance review structures that exist for other members of the Australian Public Service. That is one of the reasons we have this provision here—just to enhance that level of consistency.

PRESIDING MEMBER—Are there any other questions on section 1?

Senator MacGIBBON—The amendment then to section 90(2A) sets up purely a grievance resolution body. It has no other function?

Mr Reaburn—No.

Senator MacGIBBON—What is the meaning of the immunity from civil proceedings of any such body or person?

Mr Strang—It simply means protection from defamation actions and the like.

Senator MacGIBBON—Nothing else?

Mr Strang—No.

Senator MacGIBBON—It is not in relation to somebody breaching the ASIO Act in any way at all?

Mr Strang—No.

PRESIDING MEMBER—Perhaps we could move on to schedule 2, which is the area concerning the penalty provisions. Why was it necessary to change these provisions in the ASIO Act?

Mr Bowman—Basically, at the moment in the Crimes Act, there is a formula for converting periods of imprisonment to fines. In the ASIO Act at the moment, they are set out expressly, which means that, with time, the period in gaol and the fines get out of step. The present policy is to express penalties only as prison terms which allows the court to apply a fine if it wishes but on a formula in the Crimes Act which is periodically updated by parliament and which therefore keeps fines across the board up to date. It merely allows that mechanism to be adopted within the ASIO Act.

PRESIDING MEMBER—There is really not much difference to other Commonwealth acts?

Mr Bowman—No.

PRESIDING MEMBER—Schedule 4 deals with the Financial Transactions Reports Act 1988 and access to financial transaction information. Is it possible for the committee to get a copy of the memorandum of understanding that has been done with AUSTRAC?

Ms Montano—It is attached to AUSTRAC's submission, which was sent to the committee on Friday.

PRESIDING MEMBER—Thank you. How long is the memorandum of understanding in force?

Ms Montano—It stays in effect until terminated or varied by agreement between the Director of AUSTRAC and the Director-General.

PRESIDING MEMBER—Was it easy to change the scope of the ASIO Act to reach all those provisions, or are there aspects of the changes with the ASIO provisions that prove difficult to implement?

Ms Montano—Sorry, I do not quite understand the question.

PRESIDING MEMBER—So it was a relatively easy process for you to come to this memorandum of understanding. The fact that you were dealing with ASIO and these new provisions presented no particular difficulties?

Ms Montano—We did have an issue in the sense that ASIO is, by definition, a very different kind of organisation from the standard organisations that we deal with. So we have attached to the submission a copy of the fairly standard agreement which we reach with all the law enforcement agencies. That shows the differences quite clearly. The law enforcement agencies look at the information we hold in relation to existing investigations or they can use it for proactive investigations. We often identify stuff in relation to money trails and they follow back and find the criminal activity.

ASIO, obviously, is a different kind of animal. We are very concerned to explore, if it has access to this sort of material, in what circumstances it should have it, because, quite frankly, there were concerns about fishing expeditions. Those concerns exist in relation to law enforcement agencies, too, by the way. So we are always very careful to ensure that the kind of access is for the purposes for which it is intended.

In relation to ASIO, that has meant looking at what sort of work it does, how it does the assessment processes, and limiting access under the agreement to searches in relation to known identities only. At the same time, we had to be flexible in the sense that we found, certainly with the work of the law enforcement agencies, that because you know criminal X is doing something it does not mean that it is criminal X who is doing the transactions which are on our database. It may well be an associate, known or otherwise. It may be other information about the transaction that allows us to link it back to the criminal that they are looking for.

Similarly, we were concerned that there might be circumstances where ASIO considers something is happening; they are preparing an assessment; they are looking to find whether there are financial transactions which verify the information they have or which in some other way adds to their intelligence picture. But because we have tended in general to try to limit them to saying, `We think person X is going to do something; therefore we will search on person X's name or person X's bank account,' we are very careful to give the possibility in the document that if that does not work, they could perhaps twiddle the knobs a little and look at another angle for it, but only under very careful supervision and only if they actually ask for that particular ability to search.

We made sure that in the agreement we have drafted with the Inspector-General, of which you have a copy as well, that particular sort of request for a little bit different way of looking at the information is passed to the Inspector-General so that can be checked in the oversight processes. So we have had to try to be fairly careful about the way in which we would grant access, while also making it flexible enough so that they can use it. It is silly otherwise to have it.

Senator SANDY MACDONALD—Can you explain to the committee what AUSTRAC is?

Ms Montano—AUSTRAC is a financial sector regulator and Australia's financial intelligence unit. In relation to the regulatory role, there are certain obligations on financial institutions and others under the FTR act to identify their customers and report certain kinds of transactions. Those transactions are large cash transactions, international funds transfer instructions, international currency movements of $10,000 and over, and also suspect transactions that the institutions report to us. So that is a regulatory role, and we have a very close relationship with the financial sector as a result of that. That is referred to in our submission, because we consulted them in relation to this.

The other role is as a financial intelligence unit, and that is to provide specialist analytical support. We identify the money trails. We find the unusual patterns. We refer them to relevant law enforcement agencies, often under a National Crime Authority task force umbrella, so that they can then work up that information and go back to the crime that generated the money trails. So that is our role. Traditionally, it is a role which aids law enforcement and revenue agencies. Of course, this is a step out of that for us.

Senator SANDY MACDONALD—That is my next question: to whom are you answerable—law enforcement agencies and income tax collection agencies?

Ms Montano—When you say `answerable'—

Senator SANDY MACDONALD—To whom do you provide information proactively as a result of your sources of information?

Ms Montano—We provide information in two ways. One is the proactive way: we analyse, we refer to the agency that seems most appropriate, given what we can tell about the transactions. We only have access to financial intelligence—nothing else—which they then use to work out exactly what is going on.

The other way is that all the law enforcement agencies and the revenue agencies also have online access so they can, of their own volition, search for information in relation to particular suspects or if they are working up some particular issues. So there are a number of ways they have access which is much wider than the proposed access for ASIO.

Mr Richardson—ASIO will not have online access, Senator.

Ms Montano—Can I clarify that? I mean have online access in the sense that ASIO officers will do their own searches because it is not appropriate for AUSTRAC officers to actually be de facto ASIO officers in identifying the names and so forth. But it would not be available at the ASIO premises, which is very different for law enforcement.

Senator ROBERT RAY—They will have an identity user number each time they access?

Ms Montano—Yes.

Senator ROBERT RAY—So you will have a record each time they access?

Ms Montano—Yes, exactly. The MOUs set out the way this is done, and this is the standard for all the law enforcement and revenue agencies. Each person who is given access is nominated by their own agency. They are given a unique access code which determines the way in which they can have access. For example, a state police force officer does not. The way in which our processes work, once they log on their unique

identifier number they cannot get access to, for example, suspect transactions reports which relate to another state. We try to limit that access from the moment they log on. Similarly, the ASIO officers will not be able to use any of our macro tools where we look for whole classes of data in particular kinds of transactions—particular source countries, those sorts of things. They will only be able to access it by looking for a particular person, a particular bank account number, a particular passport number—so they are only furthering their existing information, not looking for new information that they would not otherwise have.

Senator SANDY MACDONALD—How many people have access at various different levels?

Ms Montano—It varies over time because we always go through our user access logs and delete the user privileges of those who have not accessed for a month or so. It varies between 600 and 700 people Australia-wide, so it is very closely held. It is only available, for example, in the law enforcement agencies typically to the officers who work in the central areas where the intelligence functions are, or to particular drug squads or fraud squads—particular parts. So the officers out in the Redfern police station will not have access to this information at all, except if they get it in the course of following up some particular matter. But they cannot access the database themselves.

Senator SANDY MACDONALD—This is off the track a little, I know, but I am trying to work out how you operate. If somebody went into the Redfern National Australia Bank with $10,001 in cash this morning, when does the red light start flashing?

Ms Montano—Almost 99 per cent of the reports we receive, we receive electronically. That will automatically trigger a reporting mechanism in the bank's branch so that when they enter the cash transaction over $10,000 it automatically goes to be extracted from their normal accounting processes and is sent to us overnight. A transaction yesterday should be with us today at AUSTRAC in our database. It is automatically loaded overnight, and they do downloads of batches of reports. It goes in and it is linked into every other transaction that relates to that. For example, you can then search and find that transaction, the one that happened last month, the one that happened last year and the other kinds of reports that relate to that person or that bank account. It is quite a rich database.

Senator ROBERT RAY—The whole thrust of this memorandum is that ASIO cannot go off on fishing expeditions. But what happens in circumstances where an officer accesses 40 or 50 different names which eventually, in AUSTRAC's mind, constitutes a fishing expedition? How can you go back to ASIO when they say, `Hold on—you're not even cleared on this matter; national security is involved'?

Ms Montano—We have been very careful to look at that. The question of fishing is not unique to ASIO. We have a history of managing the data and the access issues relating to it. We have audit trails which are quite precise. There are two kinds of reports that will be available to both the Director-General and the Inspector-General. The first is a very general summarised report, which we will give on a quarterly basis. We will tell them exactly which user-identifier looked at things, when they looked at them and what they looked at. Then there is a far more detailed one which will allow us to reconstruct, because it is automatically logged as they search, and will automatically recount exactly what they saw. So we can reconstruct what they looked at three months ago or six months ago.

Senator ROBERT RAY—Mr Richardson, couldn't that potentially give you a problem? AUSTRAC has the ability, by reconstructing, to know more than they probably should know. By reconstructing it you may have gone to five different individuals. That may allow someone at AUSTRAC to put two and two together—or two plus three, if it is five—to find out what you are doing.

Mr Richardson—That is a potential downside which we have to put against the benefit we are getting. I

think the equation works out pretty well.

Ms Montano—The MOUs with both the Director-General and the Inspector-General state that those records will only be available to the Director-General, the Inspector-General and me respectively and to our nominated senior officers. For example, an AUSTRAC officer—just anyone in the organisation—cannot get that information. It must be one of our senior liaison people, whose job it is to do that. We monitor those sorts of things. In the event that we have a security breach we can go back and say to the agency concerned, `Yes, we know that person X did this on a particular day and here is exactly what they looked at at that time.' It is quite precise.

Senator ROBERT RAY—If you have the memorandum of understanding in operation and you suspect that ASIO may be making too much of it, can you go directly to the Inspector-General and say, `Can you check this out?'

Ms Montano—Yes.

Senator ROBERT RAY—He has more power in this area than you?

Ms Montano—Undoubtedly, and that is why we have been very careful to ensure that the relationship with the IGIS is quite strong. A separate memorandum of understanding has been drafted—it is attached to the submission—whereby if at any time I feel concerned I can go to the Inspector-General and say, `We think there is an issue.' In any event, there is a regular oversight role. So yes, that can be done at any time. The agreement between the Director-General and myself states that the Director-General will facilitate that liaison work. So we try to ensure that there are a number of mechanisms.

The other thing is that it is quite clear in the memorandum of understanding between the Director-General and the Director of AUSTRAC that the continuation of the MOU is subject to a yearly certificate of good health, as it were, from the Inspector-General, so that when the Inspector-General reports to the Attorney-General about compliance with the Financial Transaction Reports Act and with the Attorney-General's guidelines, the Inspector-General will also provide an annual certificate to the Attorney-General to be passed on to the Director of AUSTRAC which will state that ASIO has either complied or not complied with the terms of all those requirements. If those requirements are not complied with, the MOU ceases to have effect. The onus really is on ASIO to ensure that they perform; otherwise, there will be consequences.

Senator ROBERT RAY—The question then to the Acting Inspector-General is: are there enough resources in the office to deal with this additional matter? Is it going to take much time?

Mr McLeod—Time will tell, Senator. There is certainly no concern at the outset that the office will be swamped with monitoring activity. If there are concerns about the ability of the office to meet its obligations in terms of oversight, I am sure there would be the capacity for the Inspector-General to make a submission in relation to resourcing.

Senator ROBERT RAY—I have one final question, which no-one else has asked. I do not ask it because I believe it should be so, but it will be asked in the Senate. Should this memorandum be a disallowable instrument in the Senate? Are any of the other ones with other law enforcement agencies? Is it seen as desirable or undesirable?

Ms Montano—The legislation expresses that all the agencies have access at the discretion of the Director of AUSTRAC. So the director may grant access. It has been done that way so as to allow flexibility in the

agreements themselves. So I would imagine not, because the legislation grants the Director of AUSTRAC a discretion in relation to the manner in which access will be granted.

Senator ROBERT RAY—But the argument may be put—not by me, I assure you—that because the legislation did not anticipate ASIO, otherwise it would have long ago been done, this is a flexibility that the parliament has not granted you through legislation. It was not intended to grant you this much flexibility and it should become a disallowable instrument.

Ms Montano—The legislation as it currently stands provides that all the agencies that have had access to date have access in that way. Each time we have a new agency come on board—and they come on fairly frequently every time a state body creates a new anti-corruption body or a new law enforcement agency—they are always put on the basis that they are added to by the parliament. It is an act of parliament that determines the access, not me. I do not quite see why parliament would argue it was not proper if parliament made the decision to do it.

Senator ROBERT RAY—Because the parliament has to assert itself and show that it is superior to everyone else. That is why. Some colleagues here can argue that case out on the floor when it comes up.

Ms Montano—This is an issue you will no doubt get submissions on this afternoon as to whether this is an appropriate extension of the use of financial intelligence. That is a threshold issue which obviously is not for me to comment upon. We have been looking at the implementation issues that would happen.

Senator ROBERT RAY—It is a valid question, not so much for ASIO but for some of the other tin-pot state agencies that have access. But that is a separate matter.

Ms Montano—Mr Chairman, may I point out an error in AUSTRAC's submission which I have only discovered this morning? I would not like to mislead the committee. Paragraph 6.11 of AUSTRAC's submission states that it is under the terms of the draft bill that the Inspector-General will have a certain monitoring and compliance oversight role. That is incorrect. It should have read, `The draft MOU, memorandum of understanding, between AUSTRAC and the Inspector-General'. I apologise for that error. We have just noticed it.

PRESIDING MEMBER—Perhaps we can move on to schedule 5, the Inspector-General of Intelligence and Security Act 1986. Mr Acting Inspector-General, do these amendments pick up all the recommendations from the Samuels commission of inquiry?

Mr McLeod—No, they do not. You might recall that the Samuels commission of inquiry was essentially concerned with issues that involved ASIS. Arising out of that report a range of recommendations were made to government essentially in relation to ASIS and the accountability arrangements which should apply to ASIS. One of the elements that came out of the ASIS commission of inquiry was an acknowledgment that the Inspector-General has always, since its inception, fulfilled its responsibilities in one part by carrying out inspections and generally monitoring the activities of all the bodies in Australia's security and intelligence community. But the IGIS Act had not in fact explicitly acknowledged a role for the Inspector-General in monitoring activity as distinct from the investigation of complaints or the conduct of inquiries at the request of a minister or the conduct of an inquiry on the Inspector-General's own motion.

From a formal point of view, the Inspector-General over the years has built up cooperative arrangements with the various bodies in the intelligence and security community which have permitted the Inspector-General to have full and free access to all of those bodies, which obviously is consistent with the Inspector-General being able to perform his functions fully, which has relied more on the cooperation, if you like, of the agencies

rather than on an explicit head of power in the Inspector-General act. Had the Inspector-General wished to conduct a particular kind of activity and resistance was being shown by the agency concerned and it was a legitimate concern which the Inspector-General wished to pursue, there was always the opportunity under the existing act to institute an own motion inquiry and to invoke the formal powers under the Inspector-General act going through the appropriate procedures of informing the minister and the head of the agency and so on.

With that ultimate capacity always being available, it made a lot of sense that much of the day-to-day inspection and monitoring of the agencies did not need to rely on the invoking of those formal powers. It was put into practice by the good offices and the cooperation that existed between the Inspector-General and the agencies. But with the added emphasis over the years on the monitoring role becoming somewhat more important than the responsibility for dealing with citizens' complaints, the Samuels commission of inquiry acknowledged that the Inspector-General's monitoring role was a very important one. It was felt more appropriate to make some explicit mention of that in the Inspector-General of Intelligence and Security Act 1986.

It had been intended that that would occur as part of the package of legislative proposals that came out of the ASIS commission of inquiry. But that package of proposals has yet to be put to the parliament. It was felt in government that, with some members of the community perhaps having some concerns about the extension of ASIO's powers, it would make a lot of sense to be seen to be reinforcing the accountability arrangements that apply to ASIO. Putting in the Inspector-General of Intelligence and Security Act a quite explicit provision which acknowledges the appropriateness of the Inspector-General being able to have a free hand in conducting day-to-day monitoring of the activities of all the agencies, particularly of ASIO, could be seen as another part of strengthening the accountability side of the equation in association with these measures.

PRESIDING MEMBER—What flexibility do you require now in terms of staffing levels and the particular expertise to undertake things like the financial transactions that we have just been talking about? Are you equipped to do that?

Mr McLeod—There will be the need for some training to enable us to understand the systems and the form in which the information is available for our inspection within AUSTRAC. I think the former Inspector-General has made some preliminary arrangements with AUSTRAC to take advantage of some of the training programs that are available in that organisation so that the Inspector-General's staff will be able to properly interpret the material that will be made available for inspection.

Senator ROBERT RAY—Where is the existing Inspector-General?

Mr McLeod—He is overseas on leave.

Senator ROBERT RAY—I thought that might have been the case.

Mr McLeod—He is returning later this week.

Mr Richardson—I might add something in relation to AUSTRAC. From where I sit I believe that ASIO will be very much a low volume user relative to other agencies. We will have to wait 12 months, but I think our annual reports will show that we are very much at the lower end of the usage spectrum.

Ms Montano—Given that access will not be available on ASIO premises, people certainly anticipate that ASIO officers will have to come to the AUSTRAC Sydney office—will have to make an appointment to come in—and that we will give them a room with a terminal and say, `There you are'. They will do their thing and then they will leave; they certainly will not be camped at AUSTRAC premises all the time. If so, we will have

to revisit it. We do not anticipate a high volume, simply because of the way we have structured what they can actually look at.

PRESIDING MEMBER—Other agencies have this access. Why can't ASIO have it?

Mr Richardson—The blunt answer, I think, is that it was one of the compromises that were made. Someone asked a question earlier on about the MOU: `Well, isn't that an easy thing to do?' There were a number of discussions leading up to the MOU. Given that this is new, there are understandably some community groups that might have concern about our access. As I have said before, it is absolutely essential in terms of our being able to fulfil our statutory obligations, particularly in the area of politically motivated violence.

But the concerns that some groups have are understandable, and there needed to be a range of sensible practical measures put in place that would allay some of those concerns. One of them was ASIO not having online access from its own premises. The only people in ASIO who will have access are people who are authorised by myself or by a couple of other senior officers. We will keep a register of our own people who do have access. It will be probably limited to no more than three or four people, and those people will have to physically go to the AUSTRAC office in Sydney in order to do it. It is 19th century access for a 21st century problem. However, it is worth doing if that is going to contribute towards people having more confidence in our access and the arrangements that surround it.

Senator ROBERT RAY—Does the Queensland CJC have access?

Ms Montano—Yes it does.

Senator ROBERT RAY—Does it have direct access?

Ms Montano—Yes it does.

Senator ROBERT RAY—So a tin-pot organisation staffed with misfits and with a notorious record of leaking can have direct access and ASIO, with an impeccable record, cannot. I find that a bit of a nuisance. I do not expect anyone to comment on that, but I find it a bit strange.

Ms Montano—We have benefited a lot in the course of preparing these draft agreements from the consultations that we held in 1997 and last year with two groups: what we call a provider advisory group, which is our financial sector liaison committee, and a privacy consultative group that we meet with on a range of issues, and this is one of them. The Attorney-General gave permission for me to consult on a confidential basis with both those groups when this matter was first mooted, in September 1997, with us. Certainly we have been very careful to take on board all their concerns in drafting those two documents.

Attached to the AUSTRAC's submission is the correspondence we subsequently had with those groups, particularly on the privacy concerns. I know you will have submissions about that this afternoon. We have tried very carefully to look at all their concerns and to see how we can strike the balance, which historically one has to do in relation to this material, between granting useful access but also being very careful about the privacy issues to ensure that it does not go any further than it has to. That is why we have been careful in this area.

This is very early days in relation to this for Australia. The way in which we consider the law enforcement stuff has changed over time—this is only a 10-year-old sort of concept. In years to come that may be revisited once people are more comfortable, but that would require a fair bit of review after some experience.

In relation to all those agencies, including the CJC, there are very strict audit trails in place. If, for example, there was a suggestion that there had been a leak of financial transaction reports information, we could tell you within about two or three hours whether it had come from one of their officers, which officer, when they did it, what they saw, and whether they printed it out or copied it down by hand—a whole range of things. We could tell you whether they did it or not.

That has happened, by the way, in relation to another Queensland agency—not the CJC—where it came to our attention that someone had done something improperly in relation to their own records. Within a couple of hours we were able to reconstruct the transactions that they had looked at and the copies they had made. We were able to pass that on to the CEO of their organisation for disciplinary action, refer it to the Federal Police for possible criminal action and, obviously, immediately withdraw access for that individual. The mechanisms are fairly strong. There are also obligations in the MOUs that, if they pass any information on internally, they have to keep an audit trail within their own organisations.

Senator ROBERT RAY—The point is that others have misused it and been caught. Why can't ASIO have the same access and be subject to the same penalties if they misuse? You say you can track it down within two hours. Why can't ASIO have the same rights as the CJC, which has leaked like a sieve for eight years, not just on these matters but on any matter? If they do not get their own way, they just leak—as it was proven at the commission of inquiry—to their selected, tame journalist to run the articles. I cannot understand why ASIO has been treated differently to these state organisations, given their relative track record. What would be a reasonable period for this MOU to be in operation, for that aspect then to be reviewed and renegotiated?

Ms Montano—The MOU already provides for the possibility of online access at ASIO premises. We thought about this issue and whether, after a while, we would see it was practically very inconvenient for it to be done this way. It was also a question of feeling our way and being very sensitive to the concerns. There is no reason why it cannot be rethought. This is new territory for everyone and we were trying to be very careful.

Senator ROBERT RAY—Okay. That is good.

PRESIDING MEMBER—Can I go back to the Inspector-General's role and, in particular, item 8 in schedule 5, section 34(1A). That is the area that permits the Inspector-General to refer information received to police if such information suggests a person might be at physical risk. How has this been dealt with in the past, and why is this provision necessary?

Mr McLeod—There have been occasional situations where, in the course of an investigation, the Inspector-General has had reason to believe that there may be concerns about the safety of certain individuals in the light of information that becomes available to the Inspector-General in the course of an inquiry. To be quite frank, when I was Inspector-General, on the odd occasions when that became a significant concern to me, provided I was acting properly in my view in relation to the exercise of my responsibilities and the circumstances of the case I was prepared to make certain information available to authorities so that there could be some prior knowledge of the possibility that there may be a risk.

I did that in a way that sought to protect as far as possible the passage of any information that might have national security significance, but it did involve, on occasions, the naming of an individual to other law enforcement authorities. I did not believe it would have been appropriate to suppress that material if I genuinely believed that someone's life and limb may have been at risk. I felt comfortable in being able to defend that position if I was ever called to account. But I think it would be more satisfactory if the legislation itself acknowledged that in a situation where the Inspector-General felt that a person's physical safety may be at risk, the person be given statutory protection in being able to pass on certain information to the appropriate authorities.

PRESIDING MEMBER—I move now to section 6. I apologise to the people from the Taxation Office. You have been very patient. Just to set the scene, could you tell us what personal taxation information ASIO will have access to as a result of the amendments?

Mr Mulligan—The bill provides that they can get access to any tax information that we hold on any individual or entity.

PRESIDING MEMBER—With no restrictions?

Mr Mulligan—No restrictions.

PRESIDING MEMBER—Does ASIO have direct access to that information? Does ASIO go online?

Mr Mulligan—Definitely not. The new section 3EA is drafted along lines similar to the existing section 3E, which provides for the commissioner to disclose tax information to law enforcement agencies. Under 3EA, as with 3E, we receive a request from the respective agency and, provided it satisfies the requirements of that particular provision, the tax office itself searches for the information. That agency has no access to ATO systems or officers or the like under that provision. We then hand the information over to that agency as per their request.

PRESIDING MEMBER—So in many respects the structure of your MOU is similar to the AUSTRAC arrangement?

Mr Mulligan—We and AUSTRAC are different. AUSTRAC's agency has a massive database, as the director has indicated. Under various MOUs it has with law enforcement agencies and the like, it sets up a structure whereby it regulates their access to the information held by AUSTRAC in their databases. The arrangement that we have is that we, the ATO, are the only people who have access to our knowledge, our information and our systems. When they want to receive information about a particular person or entity they give us a request. We, and not that agency, go away and search for that information and we will physically hand it over. The other agency has no right of access to our systems or information.

Senator ROBERT RAY—So no agency can go into your system.

Mr Mulligan—Correct.

Senator ROBERT RAY—Have we seen a copy of your memorandum of understanding yet?

Mr Mulligan—No. We are still working on it. It is only at draft stage.

Senator ROBERT RAY—Have you got a copy of your memorandum of understanding with the Australian Federal Police?

Mr Mulligan—Later on today we can give you a copy of our latest draft, which we are still working on, just to give you a feel for the directions in which we are heading.

Senator ROBERT RAY—Errors and omissions accepted.

PRESIDING MEMBER—I move back to section 3EA, which is the divulgence of information to solicitors and barristers who may be representing an individual. I am intrigued that that is a role for ASIO and

not for the ATO.

Ms Haly—That provision mirrors a similar provision in section 3 which relates to law enforcement agencies. We do not expect that that will be greatly used. However, we did not wish to be seen in appropriate cases, as limited by the legislation, to be interfering with those types of court processes.

PRESIDING MEMBER—So this could be done without the knowledge of the Taxation Office?

Mr Mulligan—That is correct.

Ms Haly—Yes.

Senator ROBERT RAY—Would you say that every time you grant an additional agency access it potentially could weaken the privacy and, therefore, your potential to collect revenue?

Ms Haly—No, we think that our secrecy provisions have very tight controls and are provided with penalties which are quite severe. These rights of access are not given lightly. We believe that they do not constitute a risk to the revenue but are a responsible approach to the administration of the taxation laws.

PRESIDING MEMBER—Does this really mean that some information may be able to be given to solicitors that would not normally be given to other law enforcement agencies?

Mr Mulligan—The scope of the inquiry by the law enforcement agencies and ASIO is identical.

Senator ROBERT RAY—We talked to Mr Richardson about the volume with AUSTRAC. What about the tax office? Do they have similar levels of volume?

Mr Richardson—It would be even lower, Senator.

Senator ROBERT RAY—And expires with late tax returns?

Mr Richardson—No.

Ms Montano—Can I make a comment in relation to the online access issue? Often the decision as to whether an agency will take access into their own premises is also a cost issue. To have online access in their own agencies means we have to set up communication lines, which are encrypted and so forth, and we have to make sure that we service those lines—encryption is changed regularly and all those sorts of security things. The volume is a very important question in relation to all these things. For example, some of the very small revenue agencies that have access to our information similarly do not have access in their premises, although I do not have any great concerns about that should they ask. But they choose not to do so because they feel that the number of things they want to do is such that they can deal with it by other means rather than having access on their own desktops.

Senator ROBERT RAY—But that is the case for shifting the cost to the user and for them to make the decision, rather than for you to make the decision, whether to have direct access or to fly to Sydney every second week. You should not be expected to pay.

Ms Montano—We don't, but that is why it is an issue for them in relation to whether they ask to have access in their premises or not. That is exactly right—it is from their perspective. There are a number of considerations about that.

Senator ROBERT RAY—How do you resolve potential complaints that an agency has access to a particular area and then, if you like, misuses it?

Mr Mulligan—When information comes to our attention we report to IGIS, the Inspector-General of Intelligence and Security.

Senator ROBERT RAY—You have that right to raise it directly.

Mr Mulligan—I am sure the commissioner will make sure that we do.

Senator ROBERT RAY—It is the same for AUSTRAC.

Mr Mulligan—Exactly. In relation to this MOU, we have not yet approached the Inspector-General to work out arrangements with him because we do not expect huge numbers of these cases. Hopefully, we are getting fewer problems about leaks.

Senator ROBERT RAY—How many officers within the tax office would be available for an ASIO approach? In other words, who is the approach made to, at what level?

Mr Mulligan—Under the MOU, we are talking about a nominated contact point. The actual requests will be processed by a very small number of people who will need to have the right security clearances and the like. All communication will go through that contact point and also the form of interaction in terms of flow of information, flow of paper, will be through nominated people.

Senator ROBERT RAY—What law enforcement agencies currently have access through these sorts of MOUs? The AFP?

Mr Mulligan—They are listed in section 3E of the act—the Australian Federal Police, the state or territory police force, the DPP, the National Crime Authority, the Australian Securities Commission, the Bureau of Criminal Intelligence, the Independent Commission Against Corruption, the New South Wales Crime Commission, the National Companies and Securities Commission, the Queensland CJC, and the Corporate Affairs Commission established under a law of a state or territory.

Senator ROBERT RAY—Thank you for finding that.

Ms Haly—There is also a bill before the House now that seeks to add the New South Wales Police Integrity Commission and the Queensland Crime Commission.

Mr Richardson—In respect of an earlier question about points of contact between ASIO and the tax office, in relation to ASIO, the only officers who will be authorised to approach the tax office with a request will be either me or an SES officer nominated by me. So no-one will be approaching the tax office below SES level, and in each case I will be personally authorising it.

Mr Mulligan—Just to add to what the Director-General said, the commissioner has not settled these authorisations yet, mainly because the bill has not moved through parliament. But there will also be a restricted number of people inside the ATO who will authorised to release it, in return, back to ASIO.

Senator ROBERT RAY—What relationship do these arrangements have with the taxpayers' charter?

Mr Mulligan—The taxpayers' charter sets out various standards of conduct which taxpayers can expect of us. Inside the charter there are cross-references to secrecy and to the attitude that the ATO takes towards taxpayer information. My recollection—and I must admit I did not check it before coming here—is that there is a reference inside the charter to the fact that the law permits the commissioner to pass information over to various government departments and to others in nominated circumstances. It does not articulate those circumstances, mainly because there are a number in both the Tax Administration Act and the Income Tax Assessment Act. The list would just be too long. But it does put people on notice that the commissioner is authorised in certain circumstances to hand information over for prescribed purposes.

Senator ROBERT RAY—I have some questions that I would like to ask in the wash-up section, so some time later today we can go back to them. Hopefully, that will not be long as this one.

Mr McLeod—I am not sure whether the committee requires me later this afternoon. If you do not require me, it would help me with some other obligations I have today. But, otherwise, if there are any questions that you might have of me, you might have—

PRESIDING MEMBER—We will adjourn for five minutes and have a meeting to see if we can fix that.

Proceedings suspended from 12.28 p.m. to 12.31 p.m.

PRESIDING MEMBER—After extensive consultation, Mr Acting Inspector-General, you will not be required this afternoon.

Mr McLeod—Thank you.

PRESIDING MEMBER—We have determined that there should be no in camera hearing and that the next hearing will commence this afternoon at quarter to four. I would ask that the officers be on stand-by at 4.30 p.m. Hopefully we will be able to get it wrapped up before dinner.

Mr Reaburn—Mr Chairman, we might be available from quarter to four just outside or here in the room. I take it that you would have no problems with that kind of arrangement.

PRESIDING MEMBER—That is fine.

Motion (by **Mr Jull**) agreed to:

That the following submissions as listed in the committee's review of the ASIO legislation bill 1999 be received as evidence and authorised for publication.

Motion (by **Mr Jull**) agreed to:

That submission No. 7 from the Australian Transaction Reports and Analysis Centre be received as evidence and authorised for publication but that its attachments be treated as confidential documents.

Motion (by **Mr Jull**) agreed to:

That, in consultation with the Presiding Member, the committee secretary be authorised to allow the publication of submissions to the committee's review of the ASIO legislation amendment bill 1999.

Proceedings suspended from 12.33 p.m. to 3.50 p.m.

PRESIDING MEMBER—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 and 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 Connolly—Thank you, Chairman, I would like to make some introductory remarks. Thank you also to the committee for the opportunity to present evidence today. I am here in my capacity as the director of a consumer organisation which is part of the wider consumer and privacy movement who have obviously a strong interest in the work of ASIO. I am also the nominee of the Consumers Federation of Australia on the privacy advisory committee of AUSTRAC, which was referred to in this morning's hearing, and have been following the introduction of these proposals since September 1997.

In contrast to evidence presented this morning, I will be submitting that the proposed new powers for ASIO are not justified, are not subject to sufficient controls and will have an adverse impact on privacy. In addition, I will express concerns about the impact of the amendments on the work of both AUSTRAC and the Australian Taxation Office. I note that, although a number of other written submissions have been received from privacy and community organisations such as the Australian Privacy Charter Council, Electronic Frontiers Australia and the Taxation Institute, no other community representatives have been able to attend today because of the late notice and time and resource constraints.

The ASIO amendment bill, I believe, should be read in light of certain restrictions which are in the current ASIO Act on what the functions of ASIO are and some warning bells in the ASIO Act about extending those functions. Section 17 obviously covers the current functions of ASIO, but there are two additional smaller sections. Section 17A states that:

This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent . . .

I think that is an important issue to bear in mind. Section 20 states that:

The Director-General shall take all reasonable steps to ensure that—

(a) the work of the Organization is limited to what is necessary for the purposes of the discharge of its functions; . . .

So the original legislators obviously intended the act to be read quite tightly and the powers of ASIO to be contained. The Attorney-General's second reading speech for the legislation before this committee says that the bill will not extend ASIO's functions but simply enable the organisation to meet its existing statutory responsibilities in more efficient and effective ways. We heard that message again this morning from the Director-General of ASIO, who said that this act was really just about 'tidying up' the ability for ASIO to operate in today's environment.

However, on my consideration of the bill, I believe that this bill actually extends ASIO's powers and functions to the point where it cannot be interpreted as a mere tidying up of ASIO's functions. I will now turn to seven particular matters which bear out that point.

The first matter is the new ability to obtain warrants under a less stringent test. The old section 25(1) contains a fairly complicated and perhaps badly worded test for what the minister needs to consider before issuing a warrant. There are four elements there. They are that he must have reasonable grounds for believing

that certain material exists on the premises, that ASIO requires access to that material, that the collection of intelligence by ASIO would be seriously impaired without access to that material, and that the above collection is important in relation to security. All of those four elements need to coexist before a warrant can be issued.

The new section, section 25(2), says that the minister is only to issue the warrant if they are satisfied that there are reasonable grounds for believing that access by the organisation to records et cetera will substantially assist the collection of intelligence in accordance with the act. It is actually a completely different test. The first test is a negative test: ASIO has to be obstructed in its duties before a warrant will be issued to enter premises, for example. The new test just says that ASIO must be assisted. In other words, it has gone from a test of there being an obstruction, a hindrance to ASIO—that is, if they cannot get access to these premises, the investigation will be seriously impaired—to a new test which just says that this will help them.

With such an important change being made to the test for warrants, one would expect that this would be discussed, perhaps in the explanatory memorandum and certainly in the second reading speech. The explanatory memorandum, however, makes only a cursory reference to this section, stating that the subsection simplifies the description of matters which the minister must consider. The second reading speech states that these amendments clarify the requirements for the issue of a search warrant. Then, in the Attorney-General's submission to this committee, it says that this change acts only to make the section more comprehensible.

Those three claims—the explanatory memorandum, the second reading speech and the submission by the Attorney-General—all give the message that all that is being changed is the description, or the comprehensibility, of the requirement of the test. There is no indication in any of those documents that the test itself has changed.

There can be only a couple of explanations for that. This could be a mistake, the intention could be to keep the original test and they could just be attempting to get a more plain English view. I can understand that: it took me a long time to read the original section before I could eke out the four important elements that are in there. It is badly worded. However, the test still requires those four elements and serious impairment, which is a substantially different test from the assistance test which is being proposed today.

We recommend that that section be revisited. Either we go back to the original test—and reword it a little so that it reads a bit better—or the Attorney-General's Department should be called to explain why the new test is justified and why a significant listening should be allowed. Changes would then need to be made to the explanatory memorandum, et cetera. That is the first one. I note that that was not discussed at all at this morning's hearing.

The second is the new ability to access and copy computer data. On the face of it, this is just a bit of a tidying up exercise. Computer data was not considered to be a core element when the original bill was written in the 1970s. We have here a process which is supposedly a minor tidying up exercise for the ASIO Act, but which actually delivers and resolves one of today's most controversial and burning issues concerning cryptography and the use of encryption tools by citizens and the balancing of their rights with government rights to gain access to cryptographic keys.

I am sure that some of you will be aware that there has been an international debate about things like the `clipper chip'—the ability of the US government, for example, to be able to break cryptography with the assistance of the industries which provide the cryptographic tools. Some of you may have heard of terms like `key escrow', public key authentication frameworks, certification authorities, digital signatures. These are all debates which are going on which are trying to balance the rights of law enforcement agencies with those of the public when it comes to encrypting messages.

I do not believe that this is an appropriate forum to resolve that, and I believe that the bill before us does resolve it. It makes a unilateral decision that ASIO, one agency, can have access to computer equipment, computer data, copy it, et cetera, without restriction, which obviously would include the tools for breaking cryptography, cryptographic keys. There are a number of important policy considerations before that decision should be made.

Let me give you one example which has held up for about three years now with regard to the wider debate about cryptography and law enforcement access. Let us say I am an ASIO agent and I break into your computer and manage to crack the cryptographic keys by doing that, and suddenly I have access to intelligence which beforehand I was unable to have access to. It is impossible for that information then to be presented in a court as evidence, because by cracking cryptographic keys I then have the power to have written it myself. The whole point of cryptography is that, yes, it encrypts the message, but it also authenticates it. It says that the only person who could have written the information was Joe Bloggs. Once an agency cracks the keys, they have the ability to write the information themselves, and it becomes useless from an evidentiary point of view.

That is a very important issue being discussed by the Attorney-General's Department, by the on-line counsel, et cetera. I do not think this is an appropriate forum for all of that issue to be resolved. We would recommend that, if other amendments to the ASIO Act are accepted, that particular one be deferred until Australia has a clear-cut and well articulated policy on cryptography, which at the moment we do not have.

The third issue is the ability to alter some computer data. The new powers allow ASIO to alter computer data. This to me is a complete change to the powers of ASIO. Could we ever imagine, for example, allowing ASIO to alter a document or to alter the record of a telephone conversation—the tape recording?

I think that the real reason that ASIO needs the power is perhaps to cover their tracks. Section 25(5)(c)—this is in the proposal today—will give ASIO the power to do whatever is necessary to cover their tracks, to conceal their presence. I think that section goes far enough. In other words, we say `Okay, ASIO can alter data if it is just to cover their tracks, but for no other purposes.' I would reluctantly support that ability to alter tracks in order to protect ASIO's operations. However, no other alteration of computer data by ASIO should be allowed.

When the Director-General was asked questions this morning about that section, he relied on the provisions of section 25(6) as backup. They state that, `We can't alter information if it is going to be to the detriment of a lawful computer user.' That is absolutely a diversion. No justification was presented for altering computer data except for covering tracks, and that is already in there. So we would recommend that the additional ability to add, delete or alter computer data in section 25(5)(a) should not be extended to ASIO.

The fourth point is the new ability for ASIO to gain access to AUSTRAC records without a warrant. I should state from the outset that we are completely opposed to ASIO being granted any access to AUSTRAC records beyond that which they might currently have access to through, for example, a joint investigation of the Australian Federal Police. The information collected under the Financial Transactions Reports Act must be considered, at best, incidental to the work of ASIO. The Director-General himself said, `It would be a very minor part of our activities; we would be a low volume user.'

The work of AUSTRAC in collecting information under the Financial Transactions Reports Act is incredibly privacy sensitive. You are basically collecting information from bank tellers and other cash dealers about people's personal financial transactions. Yes, it covers suspicious transaction—maybe there are not too many suspicious transactions—and, yes, it covers significant cash transactions of over $10,000. How many of us do that? But it also covers international wire transfers.

Australia is a multicultural society. We send money overseas. We support our relatives. We buy goods overseas. People have come here from a wide range of backgrounds, from countries where there may be conflict, and perhaps they are countries which pose some sort of threat to Australia or to world peace, et cetera. But those people have come here and they may transfer money back to those countries for completely legitimate reasons. Yet over time they build up a record with AUSTRAC of these transactions. It does intrude into their privacy: here is a database which holds information about their financial transactions.

The privacy movement supports the work of AUSTRAC in trying to develop privacy protections. It has a privacy advisory committee and it explains what it does over and over again to consumers. We always hammer away at them to do that, to have bigger posters in bank branches, to improve their pamphlets, et cetera. When ASIO is added to the list of users of AUSTRAC information, that has to be told to consumers. Consumers will know. The pamphlet in the bank branch will say, 'This information may be passed on to ASIO. It is a requirement of the Financial Transactions Reports Act that that be the case.' This changes the nature of those people who collect information under the act. It used to be all about money laundering and tax evasion; instead, what is happening is that, over time, more and more agencies not involved in money laundering or tax evasion are added to the AUSTRAC database users list. When ASIO is added, it adds a completely new dimension. I think a certain stigma will now attach to the work of bank tellers. It will be open for people to suggest that bank tellers are in fact de facto agents for ASIO and it will be up to the parliament, the Attorney-General, et cetera, to convince the public that there are protections in place.

So where are these protections? The bill itself is completely quiet on what the protections will be. The bill contains a few short paragraphs and basically says, 'ASIO has access to financial transactions records held by AUSTRAC.' All of the protections are then bound up in the memorandum of understanding. I am grateful to AUSTRAC for supplying a copy of the memorandum of understanding. The draft I have is dated in February to me and a small number of other privacy and civil libertarian advocates. I find the memorandum of understanding unhelpful and ineffective. We would actually seek the protections to be placed in legislation rather than in the memorandum of understanding. I would like to spend a few minutes talking through some of the issues raised in the memorandum of understanding between ASIO and AUSTRAC.

The MOU is written in an unusual manner. Clauses in there always hint at a consumer protection, a privacy protection, but are immediately followed in every case by the removal of that protection. For example, we heard today that ASIO will not have remote access to the AUSTRAC database—and that was discussed at length. That is in clause 9.

Clause 10 immediately says that if a director-general comes to the view that he would like to have remote access to the database, the Director of AUSTRAC may decide to grant it to him. This is the case throughout the memorandum of understanding. It is as though you cannot have access remotely, but you can if we agree to it. It happens with data matching. There is a clause that says you cannot have data matching, but the next sentence says that you can with the consent of the director.

We would rather see a restriction on certain activities in the legislation starting with a restriction on remote access by ASIO to the AUSTRAC database. I will come back to data matching and the bulk access in a moment. Perhaps a smaller point is that I am sure that there is no intention to allow an ex-ASIO officer or someone who has been taken off a particular investigation or case to have continued access to the AUSTRAC information which they were previously accessing only because of a specific investigation. Yet clause 14 in the MOU says that ASIO will notify AUSTRAC in writing within seven days where an officer ceases to undertake the duties, et cetera and their access will be removed. Seven days is unsatisfactory; we are in a modern age. If an ASIO officer is not authorised to access that information, AUSTRAC should remove the password that day and should not have to wait seven days before being notified about it.

What is the status of this memorandum of understanding? Clause 44 says that any variation of this MOU will require the execution of a new MOU signed by the director and the director-general. In other words, if one of the parties does not agree with what is going on, it just ceases, another one gets written and they start all over again. Clause 45 says that this MOU will remain in effect until replaced by a new MOU on the same subject matter, or terminated, and that the MOU may be terminated at any time by written notice by either the director or the director-general. It is not an instrument which is reviewable. I cannot find any appropriate regulation of this memorandum of understanding. There is no requirement for the director or the director-general to notify parliament of changes to the memorandum of understanding, yet it contains within it the restrictions which will need to be promised to the community about things like data matching, fishing expeditions, et cetera.

I turn now to my fifth point, which is the ability to gain bulk access without a warrant to AUSTRAC records. Again, it requires a detailed consideration of the MOU because there is no mention of it in the bill. There is a long clause—clause 23—which I am afraid I will have to paraphrase to you because it is a bit confusing. It says that in the course of accessing the AUSTRAC database officers of ASIO shall not download bulk information to computer disk, magnetic tape or like medium. Furthermore, it says FTR information access by officers shall not be used for data matching purposes unless specifically authorised by the director. It goes on to say that this does not preclude routine comparison by ASIO of FTR information against its existing databases, for example to confirm identities, et cetera, or the downloading of such FTR information onto ASIO internal worksheets.

This presents a difficulty because I do not know what an ASIO internal worksheet is. I do not know the operational status of some of the things mentioned in this clause, but it appears to me that this clause would allow, for example, the downloading of FTR information onto an ASIO internal worksheet without giving an explanation of what that is, and there is no explanation of how that might be different from downloading the information in bulk onto a disk or tape. It is a confusing clause. Half way through it says that there is a restriction on data matching, but immediately it says that it is okay if the director consents.

Clause 17 allows an even wider use of AUSTRAC information with the agreement of the director. It says that ASIO may from time to time form the view that it is desirable to gain access to FTR information, the parameters of which are wider than those available through the online access. It goes on to say that, with the director's consent, that can be done on a case by case basis.

That seems to me to put a lot of discretion into the hands of the director and the Director-General as to how this access actually works. We may be fortunate in that we have a good working relationship with the director of AUSTRAC but I do not think we are delivering confidence to the community about the restrictions that will be placed on ASIO's access to AUSTRAC information by putting those clauses and those protections in a memorandum of understanding, having an opt out clause for nearly every restriction and then having no process for review or even notification if the memorandum changes.

I turn now to my sixth point, which is the ability to undertake bulk data matching exercises with AUSTRAC records. Data matching is one of the bugbears of the privacy movement and is allowed in very strict circumstances under both the Privacy Act and additional guidelines on data matching. I am again referring to clause 23, the complicated clause. It does appear to allow data matching if the director consents or where the information is routinely compared against existing ASIO databases. I cannot see any difference between the general idea of data matching and the routine comparison between an ASIO database and the AUSTRAC database. I believe that the memorandum of understanding therefore anticipates and allows data matching. I am sure that is something that the community would like to know and would like to have some input on and would undoubtedly oppose. It also was not in keeping with the spirit of this morning's discussions about restrictions on ASIO access to AUSTRAC information. So we recommend that, if ASIO is granted access to AUSTRAC records, the legislation should specifically prohibit bulk access and data matching.

I turn finally to the new ability of ASIO to gain access without a warrant to taxation records. I extend an apology to the Australian Taxation Office in that, in my written submission, I have suggested that it might also be possible for data matching to occur between ASIO and the Australian Taxation Office and, having heard evidence this morning, I am not sure that that is the case. Having said that, I have not seen the memorandum of understanding or seen the regulations to which this morning's witness referred, but it is certainly our view that there should be, in legislation somewhere, whether it is in the Taxation Administration Act or within the ASIO Legislation Amendment Bill, a prohibition on data matching between ASIO records and AUSTRAC records. Again, that would be within the spirit of this morning's discussions.

It would be very important, I believe, for privacy and community and consumer advocates to see, as early as possible, a copy of the draft memorandum of understanding between the Australian Taxation Office and AUSTRAC. Taxation secrecy provisions are an incredibly important part of the overall privacy framework for Australia and if they are to be watered down or whittled away by this bill, which places no restrictions on ASIO access and which again hands over all of those restrictions and protections to the MOU, then it would be important for someone in the position to represent the views of the community to see that memorandum of understanding and to give the committee feedback on that.

I have a few final comments. One thing I would be interested in is promoting the idea that the role of this committee and parliament in considering this bill is to see beyond the rhetoric about this being a tidying up bill and to consider where ASIO is given new larger functions and powers, whether they have been justified and whether there are adequate protections. There may be a lot in the bill which is just tidying up. For example, extending the ability to get access to parcels other than those delivered by Australia Post, the ability to charge for their services and the ability to deal directly with the states for the year 2000 Olympic Games would all be important tidying up procedures. But I trust that some of those matters that I have raised today give you an indication of the strength of community opposition to some of the wider extensions which are set out and also our frustration that the restrictions and protections are dealt with in MOUs that can be changed and are not reviewed instead of in the legislation. Thank you.

PRESIDING MEMBER—Thank you very much, Mr Connolly, for that comprehensive briefing. Are there any questions from the committee?

Senator ROBERT RAY—In relation to issue one, Mr Connolly, you say that the explanatory memorandum is very inadequate when it comes to the test for issuing a warrant. We will have to follow through some of these with attorneys-general later on, but that would make it legally vulnerable, would it not, in terms of a court case because they place a very heavy reliance on second reading speeches and explanatory memorandums?

Mr Connolly—That is correct. The only real explanation is that it is a mistake, that the wording of the bill has gone too far and that the actual intention as expressed in the explanatory memorandum and the second reading speech is just to tidy up, from a plain English point of view, the original section, which is fairly unwieldy and clumsy. I think the very short reference in the explanatory memorandum is quite close to misleading. If that were the case, then a new clause would be vulnerable. The reference in the explanatory memorandum says that the subsection simplifies the description over matters about which the minister must be satisfied before he or she issues a warrant. It makes no mention that the test itself has changed.

Senator MacGIBBON—On your point about the ability to access and alter computer data, if you were here this morning—

Mr Connolly—I was.

Senator MacGIBBON—You do not accept then the explanation that the only modification of information would have been on the protective mechanisms to gain access to, not the data stored on, the computer. You reject that out of hand, do you?

Mr Connolly—My reading certainly of the clause is that a power is given to ASIO to alter computer data, to delete it or to add to it and that is quite a substantial power. The restrictions on that, as expressed by the director-general this morning, are that they cannot do anything if it would be to the detriment of a lawful user of that computer. That is how it is set out. It gives you the power, then it has this restriction. What I am suggesting is that, to deliver the intention of those who spoke here this morning and also to protect privacy, the power should not be given to alter computer data per se. Reliance should be made on a different section which says that ASIO is allowed to do whatever is necessary to cover its tracks and that would be it.

Therefore, there is no question of ASIO being given a power to alter computer data having the intention today of only doing that to cover their tracks or to gain additional access et cetera, but in the future being able to use that for a wider variety of means. It is important to consider that ASIO does collect information, and traditionally collecting information has meant copying. There has never been any question of altering, tampering or deleting information. Now that we are envisaging that for the first time, the controls need to be as strict as possible.

Senator ROBERT RAY—One of the points you made, Mr Connolly, was that it could not be presented in court from an evidentiary point of view but that would be more of a restriction on the AFP or NCA, whereas what ASIO is trying to do is collect information for intelligence purposes. So it is slightly different, is it not?

Mr Connolly—It is, certainly. I was referring to that as an example of the complications facing the wider community, which is trying to debate the balancing act between the individual rights of consumers to perhaps encrypt their messages and the needs of law enforcement agencies. We have gone through now several different technologies, trying to work out which one will deliver that balance. Do we want clipper chip? Do we want key escrow?

We are now looking at different types of new technologies and systems like public key authentication frameworks. I do not think this is the forum to suddenly give one security agency the ability to access all computer data without restriction. I do not think that has been well thought out. It surprises me, because it is the same people—the Attorney-General's Department—who have been in the muddle of the other debate about cryptography.

Senator ROBERT RAY—I am trying to narrow your objection. I do not think I have got it quite right. You seem to be saying two things, and I may not have picked them up. You are saying that it is wrong for them to access the information and then, in a further step, that it is wrong to alter it. I think you would get a sympathetic view on the altering of it, unless it is highly restricted, but what is wrong with them accessing the information?

Mr Connolly—We are slightly at cross-purposes there, Senator. I am saying that the bill allows ASIO to have access to all computer data without restriction. I am suggesting that there may need to be a restriction on that access because of another debate about cryptographic keys. If we say that ASIO has access to all computer data and we accept that that includes cryptographic keys, and in another debate some people within the security community are arguing that they do not want access to cryptographic keys, this is going too far.

Senator ROBERT RAY—But isn't the strength of that argument that, as is not the case with ASIO, if you gave law enforcement agencies that power, their very control in cryptographic equipment could allow them to

alter data that could be sheeted home to that person only? Isn't it slightly different from an intelligence gathering point of view? I can see your case much more strongly in the cases of law enforcement agencies.

Mr Connolly—There are still times when ASIO collects information with the intention of passing on that information to the Australian Federal Police for the purpose of a prosecution. Generally its purpose is to collect information but surely in some circumstances that information is taken up, and the organisation and the minister would like it to lead to a successful prosecution. But it may not.

Senator ROBERT RAY—It goes to the integrity of ASIO's collection, or the integrity of ASIO per se, that they will not alter information. You would have to be certain of that before you would think there was some case for it.

Mr Connolly—I think my point is still valid. This power is giving ASIO unrestricted access which might include access to a particular type of computer information which is the subject of wider debate and because ASIO collects information for a variety of purposes we could not rule out circumstances where they should also be subject to the outcome of that wider debate.

Senator ROBERT RAY—Let me just put one last proposition to you. Would it be valid for ASIO to access the computer information and alter it in order to gain other information from other sources? Here is an example: they are prosecuting a general investigation, they access the computer information and then use that to put queries out to other computers or other entities. Are they entitled to do that?

Mr Connolly—Is that what was envisaged by the Director-General this morning?

Senator ROBERT RAY—I do not know.

Mr Connolly—I certainly got the feeling that they would like to see—and I may be wrong about this and perhaps the Director-General will be able to speak later about it—an ability to alter records to cover their tracks or perhaps to improve their access to information. I am not sure that they wanted the ability to alter records for the purpose of generally furthering an investigation. I would take the view that we should be taking the most restrictive line on this. It can be subject to further review at another time.

It appears to me that they are only seeking quite a restricted access, and it is just the bill which is granting them wider access than necessary. The privacy interests and community interests also mean that access should be restricted as narrowly as possible. At the end of the day, that at least keeps some modicum of confidence in electronic communications and computer systems generally.

PRESIDING MEMBER—I do not ask this in a supercilious sense: have you had a go at rewriting your criticism of section 25?

Mr Connolly—No, I have not. But I did take out four elements from the clause which I believed could be expressed in the way of A, B, C and D; each of those had to be met by the minister before there was the issuing of a warrant. It certainly does read more easily once that is the case. Once you take the four elements out and list them, it is closer to plain English. It is not perfect. But I think that is where the original clause goes wrong, in that they are all jumbled together.

As I am sure you are well aware—and other privacy advocates have made such submissions to this committee over the years—the view of the privacy movement is that there is already an insufficient level of protection with there being only one minister, the Attorney-General, who is also responsible for ASIO, being the person who decides warrants rather than having a judicial officer or a committee of ministers—and there

are all those other options put about. If through this bill the problem is to be exacerbated by a lessening of the standard in that the minister applies to warrants, it is pretty serious.

Senator ROBERT RAY—At least by having ministerial rather than judicial approach here, you are able to sheet home responsibility. Attorney-Generals take very seriously the issuing of warrants. They might read some documents quickly but not those; in fact, they give them deep and heavy consideration. At least you can isolate someone as being responsible. That is not an argument against whether you should have one criterion or the four criteria you mentioned before.

Mr Connolly—I am aware of the pros and cons of the current system—

Senator ROBERT RAY—I would hate to think of their going to a committee of ministers.

Mr Connolly—and I have not made a submission today on the position either way. I am just pointing out that I am sure you are aware there is opposition to the current system. If you are then going to lower the standard, I think that opposition will resurface.

Senator ROBERT RAY—You tell us that you are totally opposed to ASIO having access to AUSTRAC, and then you put up a series of fairly cogent reasons. The weakness I find with that argument goes not so much to your reasons but the fact that other organisations of far more dubious reputation than ASIO have access to AUSTRAC.

Mr Connolly—There are two quick answers to that. Firstly, I did not say that we oppose ASIO having access to AUSTRAC information; I said that we oppose ASIO having access to information held by AUSTRAC beyond that which it can now obtain—

Senator ROBERT RAY—With AFP, sorry.

Mr Connolly—through AFP in joint investigation. Secondly, do not think for a moment that there is wide support for a number of the organisations that currently have access to AUSTRAC information. It has been an interesting history. It is an act which was proposed for one purpose: money laundering and tax evasion, and the collection of information to deal with those issues. Other people have come on board over time; we refer to it as `function creep'. It is a problem in that at some point we have to say no. Perhaps we have not had the time or resources to say no loudly enough before. Perhaps a lot of those users are not subject to the same sort of parliamentary committee that we have here today. Today we are saying no repeatedly.

Senator ROBERT RAY—I think evidence given this morning was that—and I have to paraphrase here—they are not allowed fishing expeditions.

Mr Connolly—Yes.

Senator ROBERT RAY—You are not convinced on that?

Mr Connolly—Not having read the memorandum of understanding. I can see that it is the intention of, for example, the Director of AUSTRAC not to allow fishing expeditions. But, if you read the MOU, with the consent of the director fishing expeditions can be allowed; with the consent of the director, data matching can be allowed—and some of the other problems with the MOU that I have mentioned.

If it is everyone's intention that fishing expeditions should not be allowed, that data matching should not be allowed, that bulk access should not be allowed, let's put it in the legislation. Why are we dealing with this

MOU in this way? The MOU could deal with the practical steps, the practical arrangements, between ASIO and AUSTRAC. But the restrictions, the privacy protections, the restraint on ASIO going outside its function and scope surely should be in this bill.

Senator ROBERT RAY—The only thing that I thought strange in what you have told us was your reference to the stigma attached to bank tellers. Hasn't the average punter waiting in a queue lots of things on their mind other than that the teller is a potential ASIO agent?

Mr Connolly—Every bank teller has to be trained in the workings of the Financial Transactions Reports Act, and privacy issues come up out of a range of incidents. When you open an account, you have to have 100 points, et cetera. People get frustrated; they cannot get the 100 points. They know that this is all regulated by the Financial Transactions Reports Act. There is knowledge because there are pamphlets and it is explained and there are posters at the airport, et cetera, about what AUSTRAC does and what information is recorded. Some people, although not enough, know of the $10,000 one. They also know that it has something to do with money laundering or tax evasion. Something which will really stick in their minds is if they are told that ASIO has access to their information, and they have to be told. I think that changes the relationship.

One of the things which we raised within the Privacy Advisory Committee was that we are extremely concerned that AUSTRAC issues guidelines to bank tellers and cash dealers on how to make a decision on a suspect transaction—what is `suspect'? The guidelines are very useful on that. We have to be very careful that that is limited to suspect in relation to money laundering and tax evasion, not suspect in relation to the functions of ASIO because someone is of Middle Eastern appearance or because they are sending money to Serbia. There is no guidance at the moment with those circumstances, saying, `Oh that's a suspect transaction' because it is not really a money laundering threat, it is not the Bahamas.

We are very concerned to make sure that that stays the same, that the core function of suspect transactions is money laundering and tax evasion. There is a lot of to-ing and fro-ing between AUSTRAC and the front line staff. They will have to be telling people, `This information is collected by ASIO' or `is accessible by ASIO.' It has to appear on the brochures. People forget Customs and state revenue departments, but they will remember ASIO.

Senator ROBERT RAY—But, given a choice between the New South Wales police and ASIO, I know which square they will tick.

Mr Connolly—Perhaps you and I. But, in the minds of the general public, I do not think ASIO has the golden image which may have been expressed here today because people do not know about ASIO.

Senator ROBERT RAY—That is the only point I am making: they do not know about ASIO, but they probably have a rough idea about the New South Wales police. In terms of them thinking, `Am I protected here?' and `Is this a concern to me?' et cetera, the only question I am asking is that some of the others with access would be higher in people's minds than ASIO. That is the only point I am making.

Mr Connolly—Sure.

Senator ROBERT RAY—Maybe ASIO is unlucky because it got in the queue so late. If it had got in the queue earlier, people would be arguing about state entities that are less leakproof.

PRESIDING MEMBER—Thank you very much indeed, Mr Connolly.

[4.43 p.m.]

\DB\WLBBOWMAN, Mr Norman Allan, Acting Principal Officer, Attorney-General's Department

REABURN, Mr Norman, Deputy Secretary, Attorney-General's Department

HALY, Ms Margaret, Assistant Commissioner, Law Design and Development, Australian Taxation Office

MULLIGAN, Mr Rory, Acting Assistant Commissioner, Internal Assurance, Australian Taxation Office

MONTANO, Ms Elizabeth Maria, Director, AUSTRAC

RICHARDSON, Mr Dennis James, Director-General, ASIO

PRESIDING MEMBER—Once again, could I remind you that the committee does not require you to give evidence under oath, but I should advise you that the hearings are legal proceedings of the parliament and warrant the same respect as proceedings of the House and the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament.

There is a story running around on the news wires that the Director-General, in his evidence this morning, indicated that ASIO would not be able to check fully, or check, between 40,000 and 80,000 Sydney Olympic Games workers. Could I just confirm that that is what you said?

Mr Richardson—I do not believe that is what I said. I simply make two points. Firstly, all appropriate checks which need to be done in the context of the Olympics will be done. Secondly, the fact is that not all checks will need to go to the same level of detail. Where there is a need to go beyond a basic security assessment, that will be done; where there is a need to check with our overseas liaison partners, that will also be done. The final point is: will we be operating under time pressures? We most certainly will be. That was the real point I was making this morning.

PRESIDING MEMBER—Thank you very much indeed for that answer. Evidence was given to us just a few minutes ago by the Financial Services Consumer Policy Centre. Does anybody have anything in particular they would like to come back on arising out of that evidence? Ms Montano, you were scribbling madly away in the background. I thought there might be a couple of issues arising from that evidence you would like to follow up on.

Ms Montano—Thank you. I do. We are very grateful for Mr Connolly's comments. He is a very valuable member of our privacy consultative group. As you can see from AUSTRAC's submission, we have worked very hard over the past 18 months to ensure that our approach to this issue took into account as far as possible the views of that group and the wider groups it represents.

At that group's last meeting, which was on 29 March, we provided draft copies of the MOUs between the Director-General and the Director of AUSTRAC, and the Inspector-General and the Director of AUSTRAC, to the group. We asked—in fact, pleaded—for comments. I think we add a lot of value to the process by adding their comments. Unfortunately, Mr Connolly was unable to attend due to other obligations, but I am very pleased and grateful to have got his comments today. It is always very important to test the checks and the

balances that we have put in place. There are a few things arising out of Mr Connolly's comments that we may well think are very worthwhile doing.

I was scribbling away and trying hard to note each of the points so as to be able to provide them to both the committee and Mr Connolly—who, of course, I can brief later in an attempt to put his mind at rest on a number of those issues. Mr Connolly's first comment was that his constituency was completely opposed to ASIO's accessing of the FTR information, except to the extent that they obtain information from task forces with the AFP. They do not do that at all. The way it works, for example, is that if a national security matter is being looked at by ASIO, they will have received instructions from the Attorney-General to conduct an assessment. The assessment will be done. The assessment may lead to material which suggests that a criminal offence has been committed. That would then be referred to the Australian Federal Police for investigation. The Australian Federal Police can access the FTR information themselves in relation to any investigation of a possible criminal offence.

The information does not go back the other way. Under the FTR Act, the AFP is prohibited from passing information in quite that way. Obviously, ASIO and the Director-General can comment further in relation to that relationship. But it is not quite right to say that they can get the information indirectly through the AFP. That was a comment that was made at our most recent meeting which Mr Connolly was unable to attend. So they do not have lawful right of access to any of this information, unless this amendment is made.

The second point I wrote down was that Mr Connolly has been extremely perceptive. He is not the only person who has been concerned about things like international funds transfers and the vast amount of information that is associated with them, as well as the issue of multicultural concerns. Certainly, one of the horror fishing expeditions that was put to me by a privacy advocate was whether every Serbian name was being searched. I do not think that would be a very nice idea nor is it, I think, what ASIO intends to do.

In respect of that, we have tried to look at the way in which access is granted. For it to be granted, for example, they would have to have a name, an address, a bank account number or some identifying feature. They would look in the database for something that matches that. So they would not be able to say, `Please give me every international funds transfer instruction over the past six months between Australia and Serbia, or Serbia and Australia.' That is not on.

However, we have explored what happens—and this is the scenario that was put to us, and we have worked very hard to see how we would deal with this without offending the balance—if a lawful telephone intercept is conducted as part of an assessment. Person A says to person B, `I've arranged for the finances for the arms shipment, and I have organised for the funds to have gone out a couple of days ago.' ASIO may well want to see whether person A was just big noting themselves to person B, and they will want to check whether there was an international funds transfer that fitted that description.

They may look under person A's name. It is not there. That does not mean it did not happen. It may mean that person A got another person whose identity ASIO is unaware of to do that for them. They may ask me—and this is the purpose of, I think, clause 17 of the MOU—`We've looked under person A, and it's not there. We don't think this person is bluffing; we think there was a payment. Can we check the international funds transfers between AUSTRAC and that country over the past two-week period?'

In those sorts of circumstances, we might say that that is a fairly reasonable thing to do because they are looking for something in particular; they are not fishing. There is a provision that says they can do that but only on written request, and they have to give enough information to me to know that it is not a fishing request.

Having said that, I do not want to know information I should not know. What we have done is to say `Well,

okay, we will look at that.' Unfortunately Mr Connolly did not refer to the rest of clause 17 where we have inserted a provision which says that any such request can be declined at the absolute discretion of the Director of AUSTRAC. So we have made the relationship quite clear from day one. What is more, the clause goes on to say that any such request, if granted, will be referred to the Inspector-General. So the Inspector-General, in doing the oversight role, can go back to ASIO and say, 'You looked at a fortnight's worth of international funds transfers. What assessment did that relate to, and were you just fishing?'

So I think we have dealt with that issue as best we can in the circumstances. That is why I said earlier in the day that, if government determines to give access but government also says, 'We have to be very careful about the balances and the privacy interests', there must be a practical solution arrived at. Quite frankly I think an MOU is the place to do that—subject to some other comments which I think Mr Connolly quite rightly brought up—rather than in a piece of legislation. Legislation, by definition, can be quite restrictive and perhaps does not, with the best drafting and intentions in the world, reflect all the situations that may arise. But, again, it is a matter for parliament to determine how to word that. That is one thing I wanted to say about the fishing aspect.

I am very grateful for Mr Connolly's comments on the support that we have received from our privacy group. We have worked very hard over a long period of time, since its establishment in 1993, for that committee to have a real role in AUSTRAC's work. We have certainly taken on board—I have commented upon it in our submission—matters regarding guidelines. As long as I am Director of AUSTRAC there will not be a guideline which says, `Please watch out for Arab-looking people.' In fact, over the next 12 months, it is part of the privacy group's work program to review every one of our guidelines.

We have a range of guidelines—they are only guidelines—that go out to the financial sector to try to help them determine what is something that is suspicious. So, for example, we might issue a special guideline—usually at the financial sector's request—in relation to things like cheque kiting. There is a big scam where there is a lot of fraud going on using cheques, doing round robins and things. We will do that sort of thing. We also do general ones in relation to tax havens or this or that. We try very hard to keep it fairly contemporary, but also not to be paranoid about it. At the end of the day, the decision as to whether or not to lodge a report is a subjective judgment to be made by the institution itself. There is no way that we can second guess them. So I agree with the comments in relation to being very careful about guidelines.

The AUSTRAC pamphlets, as Mr Connolly correctly points out, say at the bottom of each one of them, `This information may be passed on to law enforcement and revenue agencies.' We have already agreed that if this amendment is passed, they will also say `and national security'. Perhaps they will even say `ASIO' specifically. We usually try to keep it generic; quite frankly, if we put every agency in, we would have to keep reprinting, and that is an expensive exercise. It can also be misleading, because sometimes the institutions ask us for permission to print their own versions of our material. They hold stocks of thousands and thousands and they hand them out every time they open new accounts and so forth to explain the obligations to people. I think that is a very good point. We will be doing that in relation to pamphlets.

In relation to why none of the protections are in the bill, in terms of all the agencies that have access, that has been a historical matter. My understanding is that there was extensive debate at the time this legislation was still in bill form back in 1989 and then again in 1993 when there was a Senate inquiry into the Financial Transactions Reports Act—which was a standard inquiry—as to how this matter should be reached and how you get to a point where you can ensure reasonable and effective and worthwhile access while still protecting the privacy issues.

It was certainly decided that, because of the operational variations, geographical things, changes in the way the agencies themselves change their composition, it was important to have some flexibility but within the

context of agreements. The basis for why there is an MOU is that an MOU is in fact the embodiment of the Director of AUSTRAC's discretion. The legislation says, 'The Director may grant access.' As is usually the case where you grant someone a discretion, they form policy views in relation to how that discretion should be exercised, and that is embodied in the terms of all the various MOUs. That is why we were very keen to consult with the privacy group and our financial institution representatives in working out how that discretion should be exercised in this sort of circumstance, which is new territory. That is why I am very grateful for comments.

The comment in relation to clause 14 was very interesting. It perhaps shows that we do need Mr Connolly to come and talk to us. I am very happy to show him, with our dummy test data—under our secrecy rules, he cannot see the real thing—how the system works in relation to how they will have access. If we were terribly concerned in relation to access, the way we could deal with things is—he is quite right—take access off immediately. When he was talking I was thinking about something that we can do to the MOU—obviously, it is subject to discussion with the Director-General. At the moment we are saying that if someone ceases to undertake their duties, they are taken off the access register within seven days; that is a fairly standard thing for all the agencies so we don't have people with out-of-date clearances and so forth.

One thing we could do, for example, is every time before an ASIO officer is to come to AUSTRAC's Sydney office, we could verify with an appropriate senior ASIO officer that they are still doing assessments—something like that. I am very happy to do that. That is why we have asked for people like Mr Connolly to give us constructive comment. I think that would be an improvement to the situation.

Mr Connolly noted that clause 44 of the MOU says that if there is any variation there is a new MOU. He made the comment that if we don't agree, it just stops, and we can terminate at any time. The reality is that if that happens then there is no access—that's it. If the Director-General says to me, `I don't like this MOU,' I would say, `Well, terribly sorry.' We would try to resolve it, but the reality is that the Director of AUSTRAC—I would presume whoever is in the chair—would go back to government and say, `We have to rethink this because ASIO is seeking to change the general arrangement.'

PRESIDING MEMBER—The committee will suspend proceedings for a short time in order for committee members to attend a division in the chamber.

Proceedings suspended from 4.57 p.m. to 5.08 p.m.

PRESIDING MEMBER—Ms Montano, would you like to continue?

Ms Montano—I have just a couple more points. I think the comments that were made about bulk access misunderstand the way access will be granted in the first place. Bulk access usually means that you get a download of thousands of reports. We are very careful about data-matching with some of the other agencies—for example, the tax office and so forth—and there are Privacy Commissioner guidelines in relation to that.

I note that in any event ASIO is not subject to the Privacy Act. But usually, when talking about data-matching, the cut-off is about 5,000; certainly it is for those sorts of agencies. That may well have been an inappropriate figure for ASIO, but it is not subject to the legislation anyway. They will not be getting anything like 5,000 reports, certainly not in one hit. Apart from anything else, they will not be able to stay in my offices long enough to get 5,000 individual reports out. It is almost something that just cannot arise, given the way they will have access.

Having said that, I am very happy to talk to Mr Connolly—and obviously we have been talking already to our wider group—about how practically it will be done. I do take his point in relation to how you advise of changes in MOUs. It has never really been an issue before because of the kinds of organisations involved. I do

not know whether it is appropriate to have some kind of reporting mechanism back to some other body—and I do not wish to offend—back to this committee or back to some process whereby any changes to those agreements can be scrutinised.

Certainly, if there were any change to any of the agreements we have, the privacy committee that I convene would get those; in fact, it has seen all the MOUs and has been asked to comment on them. So I think there is a range of checks and balances in there. This is new territory, and that is why it is very important to have input from people like Mr Connolly who will gain a further understanding of what we have done.

I do not think Mr Connolly touched on the very important role of the Inspector-General. Perhaps Mr Connolly has not had the fortune of having a lot of time to look at the documents we have given him, including the MOU with the Inspector-General which shows a fairly strong role. Any time ASIO sneezes in relation to access to this, the Inspector-General will know and will be able to put it into their normal monitoring role. So there are protections in place. They can always be improved, and that is why it is very important to have input.

Mr Richardson—I would add one thing. I would simply restate that I think it is entirely unexceptional that the institution of government, which is responsible for matters relating to politically motivated violence or terrorism and espionage, should be seeking access to AUSTRAC information. Most other comparable countries around the world have that. I believe it is something of note that we do not have it rather than that we are seeking it.

In Mr Connolly's written submission, he said that ASIO's image in the general community is that of `a spy agency interested in terrorism, treason and espionage'. I would leave aside treason as it is not part of our act, depending on how you want to define it. Mr Connolly also goes on to say that `a certain stigma will attach to the work of AUSTRAC and those responsible for collecting information under the act' and that `it will be difficult for AUSTRAC to retain the current image of being focused on money laundering and tax evasion'.

I might be way off in a paddock of my own, but I would have thought that probably the community generally would not be surprised at all that an organisation with responsibility for politically motivated violence and espionage would be seeking such access. There are a variety of forms already—not in this area but in other areas—where the information collected and located down the bottom is also available for national security purposes, and I am not aware of that scaring people off. I think it is quite the reverse. I just want to put that on the record.

Ms Montano—I would also make a point—and I am very grateful to the Director-General for reminding me to make it—that certainly the colloquial explanation for what AUSTRAC is about is money laundering. But one object of the FTR Act is to facilitate the administration and enforcement of the laws of the Commonwealth and the territories. The legislation itself does not distinguish. If you look at AUSTRAC's annual reports of the past few years, that information has been of enormous help in a range of matters: exotic native bird smuggling, where the financial trails of the catchers and the sellers have lead to the offenders being apprehended; finding recalcitrant, non-paying parents through the Child Support Agency, when it was part of the tax office. That information has been used in a range of crimes where there has been a financial element.

Similarly, the states all have complementary legislation to allow reports to be lodged with the Director of AUSTRAC in relation to state offences. So when they see something coming at them they do not have to distinguish whether they think it is a Commonwealth or a state crime. So they can report without worrying about jurisdiction and getting into trouble and so forth. So, yes, it is seen as general money laundering, but financial intelligence is a much wider instrument than that.

Senator ROBERT RAY—Mr Reaburn, the first point Mr Connolly made—your department drafted this

bill—was that he was worried about the criteria becoming a criterion with regard to the issuing of warrants. Has there been a substantial change in this area?

Mr Reaburn—There has certainly been change.

Senator ROBERT RAY—Has it changed from four criteria to one criterion?

Mr Reaburn—No. There are a number of elements of the decision that has to be made by the minister. What we are talking about is the provision, the test for issue of warrant, contained in the proposed new section 25. The minister is only to issue the warrant if he is satisfied that there are reasonable grounds for believing. Both of those are present in the current act, the requirement for satisfaction that there be reasonable grounds for believing that certain things would then follow.

In the current section 25 the test then goes on and is expressed, in effect, in the negative. I think this must be one of the few, if not the only, provisions in a warrant provision where the test is expressed in the negative. The current ground is having reasonable grounds for believing that there are in any premises any records or other things. That is fundamentally replicated in the new proposed section 25. The current section states, `. . . without access to which by the organisation the collection of intelligence by the organisation in accordance with this act in respect of a matter that is important in relation to security would be seriously impaired.' So it is expressed in the negative.

The proposed new section 25 says `access by the organisation to those things will substantially assist the collection of intelligence in accordance with this act.' Then both provisions go on to say that it must be in relation to something that is important in relation to security. So there is a great deal of similarity in the various components of the test that has to be applied by the Attorney. The difference is that the central part has been turned from a negative to a positive.

Senator ROBERT RAY—Do you think the explanatory memorandum adequately reflects what you have just said here?

Mr Reaburn—The explanatory memorandum is quite short on that.

Senator ROBERT RAY—That is what I am saying. I am asking whether it is adequate in your explanation now.

Mr Reaburn—We believe that the test is a test of similar import. In that sense, what we have done is simplify the way in which the thing is proposed. It certainly does that. It is a lot shorter, for a start.

Senator ROBERT RAY—I make the suggestion that when this comes to the Senate—almost inevitably you will be putting down an additional memorandum; there are usually a couple of things to add—I would try to expand on that area, just to make it clear to the senators.

Mr Reaburn—We hear your suggestion, Senator.

Mr Richardson—Certainly, the driving force behind this amendment you have just referred to was to use plain English language to the extent possible. It was not to lower the test.

Mr Reaburn—Also in relation to this, the recourse to the explanatory memorandum and other secondary materials is, I understand, normally only had when a court feels that there might be some ambiguity in the actual statutory provision. I would not have thought that a court would regard this provision as one containing

any particular ambiguity.

PRESIDING MEMBER—Are there any other issues?

Senator ROBERT RAY—I think the one other issue we should invite would be to do with the test, and I think we have dealt with AUSTRAC. Shouldn't we revisit briefly the ability to alter some computer data, which Mr Connolly raised? Can we go over that ground again?

Mr Reaburn—There might also be some value in touching on the cryptography issues that were raised.

Senator ROBERT RAY—For the record again, could you outline what ability you will have to alter computer data and for what purpose? Let us just assume for the moment that the committee says, `Yes, we think it's fine to be able to go into computer data. It is moving along with the technological development,' but that the critical test now is your ability to then alter it and maybe later use it in an evidentiary way. What are your limitations there? Would you like to go back over that?

Mr Richardson—Subject to any correction by the legal advisers, the proposed amendments would enable changes to be made to the data re the computer in so far as was necessary to access the computer. It would not allow for any changes to the actual data held within the computer.

Senator ROBERT RAY—In other words, you can't verbal the data?

Mr Richardson—That is right.

Senator ROBERT RAY—That is just prohibited, is it?

Mr Richardson—That is right. As I said this morning, we already can access computer data in a computer through our search-and-enter warrants.

Senator ROBERT RAY—As to the question of encrypted material, do you want to add anything to what you said this morning given Mr Connolly's view that this is an area of disputation not resolved?

Mr Reaburn—I will briefly address that question of an area of disputation. It is certainly true that questions relating to cryptography have been matters of quite considerable debate across the world. I do not think that the provisions in this particular bill touch on or determine in any way the nature of that kind of debate. It is certainly true that the debate was probably given its first kick along by the United States proposal, which is referred to as the clipper chip. That was essentially a proposal that encryption would only be allowed with a government approved or government supplied encrypting device. That is, as far as I can tell, not a policy position which is held at this stage by any country in the world, particularly not now held by the United States.

The second big kick along in the international debate on this was the idea of key escrow—that cryptography would be permitted by governments but only with devices where decrypting keys were held by either a government run or a government licensed key escrow agency. Certainly my understanding is that that is not the policy of the Australian government, although there are plenty of areas where a key escrow system might be useful and valuable. But as far as I understand, the Australian government does not intend to mandate a key escrow requirement.

So there is nothing in the current either national or international debate, as I understand it, that says, in effect, that it is improper for law enforcement and/or security agencies and/or other bodies in appropriate circumstances to be allowed to have, in accordance with law, access to information which has been encrypted.

The debate has tended to be about how that access is to be obtained; in other words, how the encrypting is to be dealt with. This particular provision does not foreclose the elements of that debate.

Mr Richardson—Just to add to that, I think that the encryption issue and this issue are really quite separate. What we are essentially about here is opening the electronic door to enable us to access data. As I said, we can already do that under our search-and-enter warrant. This would enable us to do it remotely where we can. That power already exists in a number of other countries. So the encryption issue goes to a commercial issue, it goes to a security issue. It goes to the issue of how keys are going to be made available, where they are stored, whether governments have access to them. If they do have access to them, do foreign governments have access to them? It is a totally different issue from this issue.

The proposed amendments here in no way cut across and in no way foreclose the issue that is being debated with respect to encryption. That is not just an issue for Australia. There is an international forum in which Australia is part, which is also looking at that wider issue. So I think the two are really quite distinctly separate animals.

PRESIDING MEMBER—Are there any further issues you would like to raise?

Mr Reaburn—One other issue was the suggestion that if the organisation obtained access to data by cracking an encryption, this would make the data useless, because cracking the encryption would automatically mean that the organisation could then write the data itself, and that the material found would thus be unable to be used as evidence in a case.

There are a couple of assumptions in that particular suggestion. One is the fact that somebody could have altered material sought to be put in evidence is sufficient in itself to preclude that material from ever being put in evidence. I would suggest to you that that is not correct, that a court would need to examine more closely the question as to whether the material had been altered or falsified in any way before it made a ruling that the material was not admissible in evidence.

Secondly, there is the suggestion that by the process of cracking encrypted material you were therefore given the capacity to recreate it in some way; I am not sure that that is necessarily correct. The fact of the cracking might be achieved in a way that would not allow you to replicate the process which created the material in the first place. I apologise to the committee for not having enough familiarity with the mathematical relationship between private keys and public keys and the two key encryption processes to be able to give you a more precise answer. But I suspect that there are mechanisms of cracking encrypted material that do not in fact allow you to replicate.

Ms Haly—I would like to make a couple of points. Mr Connolly expressed three concerns about the powers conferred to disclose information under the proposed bill. The first two were concerns about the ability to gain access without warrant to tax records and an ability to gain bulk access without warrant to tax records. I just wanted to make the point that under proposed section 3EA(1) ASIO does not have a right of access. That proposed section provides that the commissioner may disclose information to ASIO if he is satisfied as to certain matters. There is quite a large distinction between an exception to secrecy provisions which operate by way of the commissioner being able to disclose information and another organisation having access to our records.

The second concern of Mr Connolly was that ASIO would have access to tax information via joint investigations with the Australian Federal Police. That is not the case. Although under existing section 3E of the Taxation Administration Act, under certain carefully controlled situations, tax information can again be disclosed to law enforcement agencies, including the Australian Federal Police, and under another provision to

the National Crime Authority, those organisations are prohibited from passing that information on, in particular, to ASIO. So ASIO would not have access to tax information through such joint investigations. My colleague, Mr Mulligan, will speak about the third concern, which was the ability to have bulk data matching.

Mr Mulligan—Mr Connolly raised the suggestion that there was a possibility of bulk data matching between tax data and ASIO data. As my colleague has just mentioned, they cannot get access, because we only disclose information, so there is a practical problem. There is also a definitional issue. As the Director of AUSTRAC has mentioned, bulk data matching is normally associated with bulk matching of data between both agencies. We do not anticipate that we will be receiving significant numbers of requests. If we do, we will be getting back to them to find out what is going on, because that is definitely not our understanding of the particular provision. I think the Director-General made comments to that effect this morning.

Even if our assumption is wrong about the definition of bulk data matching and there are only a small number, the reality is that we will be providing information essentially in a hard copy. If ASIO want to key that information into their system and do matching as part of their normal operational processes, that is up to them; it is nothing to do with the ATO. If it is the case that the bulk data matching is not feasible, either at a conceptual or practical level, then the suggestion that there be a regulation concerning bulk data matching is not really appropriate, because it is not relevant in the circumstances.

The final comment I want to make is that Mr Connolly asked that he sight the MOU which we are currently settling with ASIO. The Director-General and I have agreed that we will make it available once we have settled it.

Resolved (on motion by **Mr Jull**):

That this committee authorises publication of the proof transcript of the evidence given before it at public hearing this day.

PRESIDING MEMBER—I thank everybody very much indeed for the great deal of time you have given us today and the spirit in which you have answered our questions.

Committee adjourned at 5.34 p.m.