



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

STANDING COMMITTEE FOR THE SCRUTINY OF BILLS

Reference: Entry, search and seizure provisions in Commonwealth legislation

FRIDAY, 11 MARCH 2005

CANBERRA

BY AUTHORITY OF THE SENATE

INTERNET

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

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

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

SENATE
STANDING COMMITTEE FOR THE SCRUTINY OF BILLS
Friday, 11 March 2005

Members: Senator Robert Ray (*Chair*), Senator Mason (*Deputy Chair*), Senators Barnett, Johnston, Marshall and Murray

Senators in attendance: Senators Mason and Robert Ray

Terms of reference for the inquiry:

To inquire into and report on: the Government's response to its previous report on entry and search provisions tabled in 2000, entry and search provisions made since that report was tabled, including provisions that authorise the power to stop and search people, and provisions that authorise the seizure of material. The full terms of reference are:

- (1) The Government's responses to the Committee's *Fourth Report of 2000: Entry and Search Provisions in Commonwealth Legislation* and, in particular, whether there has been any resultant impact on the practices and drafting of entry and search provisions.
- (2) A review of the fairness, purpose, effectiveness and consistency of entry and search provisions in Commonwealth legislation made since the Committee tabled its Fourth Report of 2000 on 6 April 2000.
- (3) A review of the provisions in Commonwealth legislation that authorise the seizure of material and, in particular:
 - (a) the extent and circumstances surrounding the taking of material that is not relevant to an investigation and the use and protection of such material; and
 - (b) whether the rights and liberties of individuals would be better protected by the development of protocols governing the seizure of material.

WITNESSES

| | |
|---|-----------|
| GRAHAM, Ms Irene, Executive Director, Electronic Frontiers Australia..... | 1 |
| GRANT, Mrs Marion Estelle, National Director, Border Compliance and Enforcement Division, Australian Customs Service | 27 |
| GRAY, Mr Robin Michael, Acting Director, Compliance Section, Border Control and Compliance Division, Department of Immigration and Multicultural and Indigenous Affairs | 10 |
| JANECZKO, Mr Richard, National Manager, Investigations, Australian Customs Service | 27 |
| MACAULAY, Ms Louise Anne, Director, Enforcement Policy and Practice, Australian Securities and Investments Commission | 32 |
| McMAHON, Mr Vincent, Executive Coordinator, Border Control and Compliance Division, Department of Immigration and Multicultural and Indigenous Affairs..... | 10 |
| PHELAN, Federal Agent Michael, National Manager, Border and International Network, Australian Federal Police | 18 |
| PHILLIPSON, Mr Gregory Mark, Director, Entitlements Verification Policy Branch, Border Control and Compliance Division, Department of Immigration and Multicultural and Indigenous Affairs | 10 |
| WALKER, Mr Douglas James, Assistant Secretary, Visa Framework Branch, Parliamentary and Legal Division, Department of Immigration and Multicultural and Indigenous Affairs..... | 10 |
| WHITEHOUSE, Ms Anna Kirstin, Senior Government Solicitor, Australian Government Solicitor | 27 |
| WHOWELL, Mr Peter, Manager, Legislation Program, Australian Federal Police | 18 |

Committee met at 9.03 a.m.**GRAHAM, Ms Irene, Executive Director, Electronic Frontiers Australia**

CHAIR—I declare open this public hearing of the Senate Scrutiny of Bills Committee on entry, search and seizure provisions in Commonwealth legislation. The Senate referred this matter to the committee on 25 March 2004. The committee received submissions until August last year before the reference lapsed with the end of the previous parliament. This matter has again been referred in the new parliament and the committee will report later this year. I welcome the witnesses appearing today. Witnesses are reminded that the evidence given to committees is protected by parliamentary privilege and I issue the usual caution that the giving of false or misleading evidence to the committee may constitute a contempt of the Senate. I welcome Ms Graham and invite her to make an opening statement.

Ms Graham—As you received our submission quite some time ago and it is quite extensive, I really do not intend to take up your time going through all of that again. All of our concerns about the search provisions in the particular pieces of legislation we referred to in our submission still exist. Some of those, we feel, are even more problematic now because two pieces of legislation were passed by the parliament last year, in particular the Telecommunications (Interception) Amendment (Stored Communications) Bill.

As we raised in our submission, we are very concerned that now that stored email and voice mail messages are not protected by the interception act, there is quite possibly the potential for content of email and SMS messages to be able to be obtained by a wide range of government agencies without a search warrant under the pre-existing provisions of the Telecommunications Act 1997. Of course, we are aware that the government have said they are going to relook at the interception legislation this year, but I would like to flag that we do feel there is a real problem with the provisions of the Telecommunications Act 1997 in terms of access to content of communications because of the changes to the interception act—that now any protection for those types of messages under the interception act has ceased, so there is a much broader access regime under the Telecommunications Act. We really think that both of those pieces of legislation need to be looked at.

There have been no further changes in relation to our concerns about computer searches and Anton Piller orders. I would perhaps mention to the committee, if you are not aware of it, that there was quite a comprehensive paper published in the *Australian Bar Review* in November or December, discussing privacy and Anton Piller orders. The author of that article suggested a number of things that could be done in terms of the way the court issues orders in order to protect the privacy of third parties who are not suspected any wrongdoing but whose communications and other personal information may be caught up in these vacuum cleaner type approaches when universities and ISPs' premises are raided by civil litigants. Just in the event you might want to look at that article, it is titled 'Privacy v Intellectual Property litigation: preliminary third discovery on the Internet' by Nic Suzor. It is in volume 25 of the *Australian Bar Review*. You may be aware of it but it is a very good article that covers in even more depth what the issues are with that particular type of order that is currently being issued. That brings to a close my opening statement.

CHAIR—We around Parliament House have detected a major problem with the issuing of warrants against electronic databases, where everything is swept up under either a fishing expedition or an inadequate knowledge of what is there. Isn't this partly the fault of magistrates that issue warrants?

Ms Graham—It would certainly appear to us that that is the case. One, unfortunately, is left to wonder whether magistrates are aware of specifically what it is they are granting access to when they issue these very broad orders. In that article I was just mentioning that was in the *Australian Bar Review*, the author discusses a case in 2003, *Sony v University of Tasmania*, and he remarks in that article—I do not think I myself have seen the transcripts of relevant parts of that case but this person obviously has—that the access to a broad range of personal information was recognised by the judge at the time the order was issued, because he said that the accessed material 'will include a great deal of extraneous and irrelevant material' including material 'which may be privileged or subject to confidentiality obligations'. Nevertheless, this broad order was granted and it was basically left to the University of Tasmania to come back to the court later and try to claw back what information was going to be given to the litigants. We do not know what the outcome of that case is because, even though that Anton Piller order was issued back in 2002 or 2003, that case, as far as I am aware, has not actually come to trial yet.

You have to wonder about these kinds of cases. Anton Piller orders are supposed to be issued for urgency reasons, because there is danger that material might be overwritten by computer functions or whatever. You have to ask whether the idea was principally a fishing expedition, when the order was issued in 2002 or 2003—I cannot remember the date, but it was certainly pre mid-2003—yet I have seen nothing further in the Federal Court in terms of a trial about this. Obviously all this information has been collected, so what is going on?

We really do feel that there may be a need for the court, in particular—and we have not really looked into the extent to which legislation might deal with this—to review its practice notes. As I think we mentioned in our submission, the Australian Law Reform Commission mentioned in a report in 1995 that the court's practice notes on Anton Piller orders should be further extended to deal with computer searches. But the court's practice notes have not been changed since 1994, and of course since 1994, as you have just mentioned, there are vastly more computer databases and things. Technology has gone way ahead. Basically, we feel that the court needs to deal with this through either further practice notes or rules of the court that provide some principles and guidelines as to what type of information can be accessed in what circumstances. Failing that, we wonder whether the time has come to review the Federal Court of Australia Act to pull in the powers of the court in that regard or, at the least, make it aware that it really needs to give more consideration to the information of uninvolved third parties that it is granting access to.

It is particularly concerning to us when the content of computers is being handed over to the litigant's forensic experts or lawyers. Basically irrespective of what the court says, there is really no protection for the information. The court will not know whether those people have misused the information or given it to somebody else or will do so at some time in the future, and as far I am aware there are no requirements to have the information deleted. Even the Federal Police under warrants are required to delete information that is not necessary for an investigation after a period of time or if it is found that it is irrelevant. But civil litigants seem to be able to get access to information through the courts, with no accountability or regulatory requirements to ensure that the information is subsequently deleted and not misused. We feel that is a massive problem.

CHAIR—And the only redress at the moment, if you believe that what has been seized has no relevance to the warrant, is for you to go back to court and reargue the case.

Ms Graham—That is right. The respondent has the opportunity to phone the court at the time the order is going on and argue about it, but if they do that they run a risk that, if the court decides there really is no problem with this search, the respondent can be found to be in contempt of court at that point. Even apart from that, what we see as a serious problem is that when the search is being undertaken—for example, at the premises of an internet service provider or a university—the information that is being seized will include information about third-party customers or students. You have to ask whether an internet service provider or a university are going to be willing to spend sufficient time, money and effort to go to court and fight for the right of their third-party customers, who are not suspects. If my ISP is raided and information about me is collected, I do not have an opportunity to say to the court: ‘Hey! My information should not have been collected in that raid.’ I just use myself as an example to try to make this clearer. At the end of the day, it would have to be my ISP who were willing to spend their time and money saying to the court, ‘We don’t think all of our customers’ information should have been collected.’ That is another problem, we feel, because these Anton Piller orders are no longer being issued just in relation to the respondent in a particular case; they are being issued to service providers and so forth, so there is vastly greater potential for third-party evidence to be swept up.

CHAIR—To what extent do you think there is evidence that, in sweeping up so much information not even relevant to the case, they are economically damaging the person from whom the information has been taken because it cannot be used in their business or profession for that period?

Ms Graham—Where it is a computer search, they would most probably still have the same information because they are going into the premises and basically taking entire copies of the hard drive, but they are not actually taking the computer equipment away. So the respondent would still have access to the same information because they would still have the computer, the server—whatever you want to call it: the computer equipment with the hard drive on it—it is just that someone else has got a complete copy of that. Of course, in terms of commercial issues, one of the issues with Anton Piller orders has always been that, in effect, the litigants to whom the order is issued, who end up with the information, can potentially end up with commercial-in-confidence information about a competitor. That has always been a major issue with the Anton Piller orders.

The courts are aware of that. When it is a raid of commercial premises, there seems to be, from a few reports that I have read, more attention to this issue of commercial-in-confidence and whether it is really a fishing trip to try to find out about competitors and that kind of thing. It would seem to me that, basically, because these kinds of orders have been issued for many years, the commercial issues are being recognised by the court. But, on this whole area of raiding universities and internet service providers where there are third parties who are ordinary individuals, I get the feeling that the courts have not come sufficiently to grips with that issue, and it is simply not being paid enough attention to.

I would say the same thing applies to the particular case of a senator's office. There are real questions about whether courts, for example, consider enough about parliamentary privilege and so forth when they are issuing some kind of order. It is a worry.

CHAIR—We are ever vigilant and we are on the job on those issues, I assure you. A harder question, I suppose, and a more basic one of law is: who judges judges and magistrates in issuing a breadth of warrant? How can that be measured, and how can we change behaviour when there is a degree, quite properly, of independence for the judiciary?

Ms Graham—We agree with that entirely. It is a real problem. To some extent, perhaps it really does boil down to the need to just increasingly raise these issues and hope that the message gradually gets through to the judiciary. It is obviously difficult for parliament or anybody else to try to interfere in the workings of the judiciary, because you obviously do need an independent judiciary and they obviously do need discretion. I really feel that the question for me is: how can one convince, for example, the chief justice of the court that their practice notes need to be revised so that there is more transparency to the public to see that the court recognises these issues and is trying to deal with them? A further problem with the Anton Piller orders in terms of—

Senator MASON—What do you mean by the practice notes? Do you mean in terms of the court's processes or the outcomes?

Ms Graham—The court has an actual practice note in relation to the issue of Anton Piller orders which sets out a range of conditions and principles about in what circumstances Anton Piller orders should and should not be ordered and so forth. They have a number of practice notes on various issues, and they are on their web site. You can quite easily go and see them. The problem that I am raising with those practice notes is that, whilst they are very good insofar as they go for certain types of things, they just do not cover issues about broad collection of computers and—

Senator MASON—Contemporary relevance.

Ms Graham—That is exactly right. They need to be updated. As I say, the ALRC recommended that they be updated back in 1995, so it is a real concern that nothing has happened. I feel that there is even greater occasion for public concern because, firstly, the public can see those practice notes and see that there appears to be no attention being paid to these issues.

Secondly, the court's reasons for granting the Anton Piller order et cetera do not appear to be ever made public. Some are, but very few. When I say 'made public', they certainly do not end up on, for example, the Austlii law site, where almost all of the Federal Court judgments are put. But judgments—decisions—in relation to issuing an Anton Piller order seem to be very rarely made publicly available. It is the same with orders made under state legislation. Occasionally, but very rarely, you can find the court's reasons for granting a particular order. I do not know why this is. Because orders are always issued for a surprise raid, at the time the order is issued it is sealed, as there is to be no notice to the respondent that their premises are about to be raided. Further, it appears to me that what may happen is it may never get unsealed. So, even though the raid is finished and the case has been to court and so on, it would appear—I am guessing—that

the decision remains sealed. To me, this increases the level of concern, because you cannot even read the reasons for why these orders are being issued to see the extent to which the issues about computer searches and third parties are being taken into account.

Having said that generally you cannot see what these orders are, certainly we have seen some. One that was issued last year ended up being presented in a court case that is before the US courts, and the relevant legal people in that instance have been publishing all of the applications and submissions and so forth on their web site. So you can go to the web site in America and find the full details of the Anton Piller order issued in this case in Australia. You can certainly see that the way the order was written gave vast potential for third-party information to be caught up. There did not appear to be any attention paid to the privacy of third parties in terms of the computer information other than 'It has to be given to the forensic experts, and they're not allowed to use it until we have further discussion about this in court.' But the point is that they still have the information, and you do not know what they are doing with it.

CHAIR—When you say you do not know what they are doing with it, do we have evidence so far in any of these cases that the information has been abused and misused?

Ms Graham—We are not in a position to know that. But with recent raids that have been occurring in relation to the music industry you certainly do have to wonder whether—if they are ending up with information about a lot of individuals on the internet that is caught up in one particular investigation—it is being subsequently used to investigate those individuals who were not a suspect at the time that the Anton Piller order was issued. Because of the potential for that, this is why we have concerns.

CHAIR—It does not weaken your case at all, but if there are actual examples we need to know.

Ms Graham—We have not heard of any. One issue not just in this particular instance but even in the Privacy Act, for example, is that it is very difficult for individuals usually to know whether their information is being misused. It is not until some sort of catastrophic event occurs that you realise it is being misused. The real issue with trying to enforce privacy regulations is that you do not necessarily always know that it is actually happening. That is why we need laws to try to discourage misuse in the first place.

Senator MASON—Your details have been sold to commercial enterprises.

Ms Graham—And you have no idea that they have. Even if you find out or it is plain to you that your silent number or something has been given to somebody and is being used, you usually cannot track down how they got it. Although it may be quite evident that information is somehow being passed on, you cannot track down who did it. All you can say is that obviously someone has disclosed it. The same kind of problem exists with the Anton Piller orders: it is odds-on you are not going to know. Eventually, there may be cases where someone will be able to identify that that information must have come from somewhere like that, but whether it will ever come to public light is hard to say.

Senator MASON—The chair's questions focus on the broad issue. It seems to me that the law relating to search and seizure and entry was developed when, in the case of commercial

enterprises, there were files in decentralised locations. What you are saying is that has all changed with the development of computers and so forth and the law has not changed to reflect that. In a sense, privacy concerns are heightened now for two reasons: one, because of the technology and, two, because of the increased threat we now feel with respect to terrorism and so forth. In other words: the threat to privacy has increased because of technology and also because of the increased threat from terrorism and so forth, and yet the protection of the individual has not. Is that a fair summary?

Ms Graham—Yes, that is basically right. Things seem to be going too far; the threats seem to be completely reducing the balance that basically used to exist between protecting privacy and the legitimate needs of law enforcement agencies—or even civil litigants for that matter. But the fact is that things are now in computer databases or on computer hard drives and it is becoming increasingly easy. In the concern to ensure, for example, that police have the information they need, a vast range of other information is potentially caught up.

Senator MASON—Yes, but, to use your term from before, you have to go driftnet fishing to get that information.

Ms Graham—Yes. I really look at the issue of computer hard drives. You can compare them to, for example, a set of filing cabinets in an office. Generally speaking—certainly in the case of Anton Piller orders, but quite probably in relation to most search warrants—it would be fairly rare that you would go into somebody's home or office and taking away 100 filing cabinets from along the wall, and everything in them.

Senator MASON—You might take three away.

Ms Graham—Yes, but you would not take the whole lot. Now everything is on a computer or on several computers and it is on a hard drive and because it is so easy to download everything that is on the hard drive and take it away, that is what is happening.

Senator MASON—I was reading this morning the Australian Federal Police submission, and they are quite frank about it. They say:

Since the Fourth report was tabled in 2000 the criminal environment has changed significantly and this reinforces the necessity to expand current legislation to meet new challenges.

Does it?

Ms Graham—Certainly that is what has continuously been said.

CHAIR—But they do not actually go on to say what new scrutiny measures they want for these increased powers.

Ms Graham—Yes, that is right. We can accept that there may well be cases where, for example, the Australian Federal Police do need increased powers, but we get very concerned when the arguments that are being put forward do not seem to justify the powers that are required and there is no relevant accountability and there are no transparency measures that seek to ensure the new powers are not abused. That is a principal issue we have with the stored

communications situation under the interception act. Basically all of that has been completely removed from that act, but no accountability measures and no related procedures have been put in place to limit the breadth of the effect of the changes. In the past, if that kind of information had been accessed under the interception warrant, there was a requirement to report that to the Attorney-General's Department—it probably wasn't the Attorney-General's Department; I think they had to report it to the ACA and the ACA reported it to somebody else. Anyway, you would end up with an Attorney-General's Department report in parliament as to how many instances there were and how many instances led to convictions and so forth. There was a requirement for there to be publicly available information about the usefulness of these kinds of warrants.

So we have just removed one complete set of information and there is absolutely no way now to identify whether, when those new powers are being used, they are actually succeeding—not necessarily in reducing crime but in catching criminals, basically. There is just no information there to enable one to know. And that is often the problem with the seeking of the new powers: either it does not appear on the face of it that the new powers are actually going to give very much greater power in terms of successful outcomes—that is, it does not appear that what is being claimed matches the powers wanted—or alternatively, even if the powers are perhaps legitimately needed, where are the measures for accountability and so forth that go with them?

Senator MASON—You said in evidence before that perhaps the practice notes of the Federal Court should have been amended since 1995, when the Australian Law Reform Commission said that should be done. That was 10 years ago.

Ms Graham—Yes.

Senator MASON—Technology has obviously changed so much, even in 10 years, and the threat has changed enormously since September 11, so the powers have been increased and technology has increased to enable greater search and seizure and so forth. Yet, as the chair said, we are not sure we have the accountability mechanisms.

Ms Graham—Yes, that is right.

Senator MASON—In summary.

CHAIR—I will have to correct you. The threat has not increased since September 11; it has just become more apparent. More is known about it.

Senator MASON—The former defence minister is speaking now.

CHAIR—Well, that is more accurate.

Ms Graham—I agree with you, but it is difficult to keep saying to people: 'Has the threat really increased?' But certainly we agree that there is a level of panic that perhaps does not justify quite—

CHAIR—You are not actually agreeing with me at all, but we will not go into semantics. Finally, I ask: for all these technological developments and then the countermeasures, Anton

Piller orders et cetera, is there a nasty group out there developing technology to counteract the effect of these orders?

Ms Graham—Sorry, I do not think I quite understand your question.

CHAIR—For instance, what would happen if, the moment I hand out my hard drive to someone other than myself, all the information disappears, dissolves, off it? We have had problems not only with the encrypted stuff on the hard drive but where the dope that put it there has forgotten the code so we are never able to break into the files. It is not deliberate; it is just an accident.

Ms Graham—Yes, but you can be sent to jail for six months if you have forgotten the password, if it is a crime.

CHAIR—Well, he is going out on June 30 anyway!

Ms Graham—Did you not know that?

CHAIR—No, I did not know that.

Ms Graham—It is under the Cybercrime Act 2001, and a section that provides for what are called ‘assistance order provisions’ has been incorporated into the Crimes Act 1914. An assistance order entitles a magistrate to order a person to hand over their—

CHAIR—Yes, I knew that, but I did not know that if you had accidentally forgotten it you could be strung up.

Ms Graham—Basically, we believe absolutely that, yes, if you have forgotten it, you could end up in jail, because there is absolutely no defence to this order. If you are ordered to provide assistance in terms of either helping them access something on a hard drive or giving them a password or an encryption key, if you do not comply with the order the penalty is imprisonment for up to six months, and there is absolutely no defence to that.

CHAIR—I will check back to see whether the previous Scrutiny of Bills Committee picked up this terrible thing.

Ms Graham—I do not think they would have, because it was not there then. This was implemented in the Cybercrime Act 2001, and I think this committee’s last report—

CHAIR—The Scrutiny of Bills Committee has been around since the 1980s.

Ms Graham—You meant just in that bill?

CHAIR—Yes.

Ms Graham—I was thinking you meant the committee’s previous report.

CHAIR—We will check that.

Ms Graham—We certainly had concerns about that. We raised it before the Senate committee that inquired into that bill and pointed out that, at the very least, if it is claimed that you cannot be sent to prison for this then there needs to be some provision in terms of how you would ever prove that you had just forgotten the password or that the hard drive or something that you had kept it on had had a technological problem and it had just had errors on it.

Senator MASON—No need to prove criminal intent; I understand.

Ms Graham—Yes, that is it. One would hope that the criminal intent issue would be taken into account, but we do find it very concerning that this was the case. Even worse than the actual provisions in the Cybercrime Act—and I think we did mention this in our submission—is that part of the Spam (Consequential Amendments) Bill 2003 that amended the Telecommunications Act 1997. These same assistance provisions are in the spam bill. The situation now with the spam bill is that, if an Australian Communications Authority spam inspector—who is not necessarily a police officer—decides to go and investigate whether someone has been sending spam and there is something on that person's computer that is encrypted or password protected, the inspector can get an assistance order from the court to require that person to hand over their password or encryption key. If they refuse to do so or they have forgotten it or they cannot do so, there is a six-month imprisonment penalty. However, even if they are found guilty of sending spam, it is not a criminal offence and there is no imprisonment. Even if a person is found guilty of sending spam, they cannot be sent to prison—but if they are suspected of sending spam but have forgotten their password they can end up in jail for having forgotten the password. We find that completely absurd.

We do not think you should have penalties for forgetting a password that can potentially land someone in jail when they are not even suspected of a criminal offence in the first place. We felt this provision was way over the top. It seems to be a case of 'we'll develop one provision in relation to computers for one type of law and then for every other law that we make that has anything to do with computers we'll just copy the provisions across and we'll not even stop to think of whether this is a criminal law that we are developing here or a civil law'. I am pretty sure that the Scrutiny of Bills Committee did not mention that. I think they were probably too busy at the time.

CHAIR—They were probably looking at 55,000 ASIO bills. Thank you, Ms Graham, for your evidence this morning. You have helped to elucidate quite a few of the issues, so thank you for your attendance.

[9.38 a.m.]

GRAY, Mr Robin Michael, Acting Director, Compliance Section, Border Control and Compliance Division, Department of Immigration and Multicultural and Indigenous Affairs

McMAHON, Mr Vincent, Executive Coordinator, Border Control and Compliance Division, Department of Immigration and Multicultural and Indigenous Affairs

PHILLIPSON, Mr Gregory Mark, Director, Entitlements Verification Policy Branch, Border Control and Compliance Division, Department of Immigration and Multicultural and Indigenous Affairs

WALKER, Mr Douglas James, Assistant Secretary, Visa Framework Branch, Parliamentary and Legal Division, Department of Immigration and Multicultural and Indigenous Affairs

CHAIR—I welcome Mr Vincent McMahon, Executive Coordinator, Border Control and Compliance Division, and other officers of the Department of Immigration and Multicultural and Indigenous Affairs. I do not need to remind Mr McMahon of his duties as a witness, as he has been before many of these committee hearings before and has the corporate knowledge of the department. If any of the other witnesses want to make a contribution, I invite them to do so. I invite you to make any comments that you have prepared to help elucidate these issues.

Mr McMahon—I looked at our last submission, which was made in only June last year, and I do not have a great deal to add to that. What I thought might be useful, in looking through the reports, would be to table some updated data for that submission. I also thought it might be useful to table the information sheet that we hand out to people when we are serving warrants. It is in 15 languages or so. I thought I might also refer to what I see as the three key developments since the committee's original report.

One of them was the issue of a comprehensive instruction on entry, search and seizure, which we put very considerable efforts into producing. We also issued operational guidelines and developed a major training program, which we have been running. Included in that training program is a focus on entry type issues. It is probably worth noting that the instruction actually limits the powers given to us under the act. In particular, the powers in the act are relatively open in respect of the issuance of the warrant—as opposed to the serving of the warrant. Essentially, what we have done is to impose on the issuance of the warrant the same conditions that exist on the serving of the warrant. The act also allows the warrant to be open for three months. As a general policy condition, we have required that the warrant only exist for seven days, although there are some limited exceptions.

The only other thing that I want to note is that we have been in relatively close contact with the Ombudsman in recent times. You may know that the Ombudsman decided for this year that one of his focal points will be our warrant issue and administration. Consequently, I have had some discussions and I have also invited some of the senior members of the Ombudsman's

office to attend compliance actions so they can see the entire process and look at the warrants themselves. We are also undertaking some systems work which we hope will increase the level of documentation around warrants and also require people to respond to all the questions that we have raised as a matter of policy within our instruction.

CHAIR—The number of warrants has eased up a little over the last four or five years, but not massively. I assume if you projected the 2004-05 figures just by doubling them then that is a fair enough guess, isn't it? Or do you have particular seasons?

Mr McMahon—You could say that they are going to come out broadly of the same order. It has been a reasonably stable number over the last two to three years.

CHAIR—What are the main circumstances when issuing a warrant?

Mr McMahon—Probably half the circumstances would be that we get information relating to a person who is believed to be working illegally or whatever. We then undertake some checks. For example, there is no use getting information which says that there are Korean tilers working on a building site and when we look it up on the web the building site is only at the stage of digging the footings. We would not attend. We normally look for some level of verification. It could be the history. Particularly in respect of brothels, for example, we would look to see whether or not the person had a history of employing illegal workers. We might also look to see whether an employer was checking against our systems to see whether or not the people were legal. Once we form a picture, the person requesting the warrant, under our policy, must form a reasonable cause to believe that there is either a person there who is working illegally or an overstayer. A warrant request is made. The person who then approves the warrant then needs to be satisfied that the person has formed a reasonable cause to believe. The warrant is then served and, at the time, the person serving is required under the act to have formed that belief as well.

Normally there is quite a bit of preplanning. What sometimes looks to be overkill on our part is because, from an operational level, some of the places we go into are inherently difficult to manage. There may be multiple entrances or we may have information on workers but not know where they are. So we tend to do a fair bit of planning and, over time, particularly if we get repeated requests, we keep a corporate knowledge of the layout of the institution or whatever it is and refine our processes.

CHAIR—Do you think it is a more difficult area for your group, compared to many other government agencies? You are dealing with a far more emotional and reactive area than even the Federal Police dealing with criminal elements et cetera.

Mr McMahon—There is a range things we need to take into account. First of all, we are to assess whether or not we require police on the job. Obviously, if you have police on the job, were there a threat it is much more easily managed. In general we would simply withdraw if there was any real threat and we did not have support. The level of emotion would vary quite significantly on the jobs. Quite clearly, people are sometimes distressed. They know they are working illegally and that they should not be working. Nonetheless, that may be the only opportunity in an individual's lifetime to get their head above the pack if they are from, say, China and in poverty. So it is quite distressing for them. You also do not know the background—

whether they may be in debt as a result of having come to Australia. In general, though, I would have to say that there is not a great deal of emotion.

Managing the business owners can be a bit of a problem at times. They quite clearly want to get on with business, and sometimes that can be quite dangerous. For example, I was recently in Melbourne on a compliance action. We went into a restaurant where two or three people were working illegally. The person refused to turn off the cookers. We were in a slippery kitchen and they continued to cook until we ordered them to turn off the cookers. Nothing sharpens the mind more than being about two feet away from a boiling pan of oil.

CHAIR—There was a famous case involving kitchen staff 17 years ago, when my state director was having his wedding anniversary out the front and you got the kitchen staff in the back.

Mr McMahon—That one I do not know.

CHAIR—The illegal waiter whipped off his apron and sat down and had a meal with him. In what circumstances are officers empowered to seize materials or documents without a warrant?

Mr Walker—There certainly are some powers. Most of them specifically relate to the boarding and searching of vessels. On land—in buildings and so forth—there are limitations. On land, the only area where we can seize documents, materials and so forth is in relation to detainees. We have some powers in relation to the searching and seizing of property in their immediate possession.

CHAIR—Whilst under detention?

Mr Walker—Yes, whilst they are immigration detainees. We also have powers to ask persons visiting detention centres to empty their pockets. It is not so much ‘seize’ but retain items which we believe would constitute a threat or danger within the detention centre or—

Senator MASON—Can you search visitors?

Mr Walker—No. We can ask them to undertake a screening process, empty their pockets, remove a jacket, but we cannot do the traditional ‘pat down’ search of a visitor. A better way of describing would be that we can retain those items while the person is visiting the centre. The items must be returned on their departure from the centre. So it is not seizure in the sense that I think you are looking at.

CHAIR—So it is mostly on vessels.

Mr Walker—It is mostly on vessels. That is right.

CHAIR—Are they vessels at sea or can they be in port?

Mr McMahon—They can be at port or at sea, yes.

Mr Walker—Section 251 deals with vessels, and that power in subsection (1) and (2) is predominantly about vessels in port. There are other provisions relating to stopping the movement of a vessel for a limited period of time while you search in port. Division 12A of part 2 of the act deals with the boarding and search of vessels at sea. That division was put in specifically to deal with people-smuggling operations.

Mr McMahon—Before we can exercise that power we must reasonably suspect. There is no legislative definition of that, but our instruction says: ‘Reasonable suspicion requires the existence of facts sufficient to induce suspicion in the mind of a reasonable person. However, a reasonable suspicion is more than a bare possibility. It is a positive feeling of actual apprehension or mistrust on the information available rather than mere speculation.’

Senator MASON—It is a formulation of common law, isn’t it, Senator Ray?

CHAIR—You would know better than me.

Senator MASON—I think it is.

CHAIR—In what circumstances can material be seized which is unrelated to the warrant that you are searching on? When you go in on a warrant to search for material, do you have any capacity to seize other material?

Mr McMahon—We have very limited powers. We have very good powers, from our point of view, of going in. Once we go in, our powers are very limited. We can obviously take into detention a person who is working illegally et cetera, but the limits of our power to acquire material relate to the identity and status of the person. Even if we saw, for example, narcotics or—

CHAIR—Let us use this example: you want to see a person’s passport and you see another three or four dodgy looking passports there.

Mr McMahon—Yes, we would have the power, I believe. I will need some legal advice on this. Essentially, if we saw something that led us to believe that a document relating to travel was fraudulent, we do have powers under 189 in respect of that. If we went in there and, even if it were not related to the warrant, we saw a person about whom we formed the view at that time that they were an illegal, it would not be the warrant that was providing the power; it would be the act itself.

Senator MASON—I see.

Mr Walker—Predominantly, it is quite specific to immigration related matters. The power of seizure that goes with the warrant is very much conditioned on the basis of ‘may seize any such document’. Reading on in the act, it is about entering, with the warrant, the premises where you have reasonable cause to believe that you will find:

(d) any passport or document of identity of, or any ticket for the conveyance from a place within Australia to a place outside Australia of, an unlawful non-citizen, a removee or a deportee, within the meaning of the Act;

and to seize any such document, book, paper, passport, document of identity or ticket, as the case may be, and to impound and detain it for such time as the officer thinks necessary ...

That is the power. It is quite specific in the circumstances, going to identifying the individual and determining status and, if necessary, facilitating their departure. Obviously that is what the ticket is for.

The power in relation to vessels at sea is a little bit broader. It is securing any goods found on the ship or the aircraft, requiring persons to produce any documents in their possession that go to identity or are related to a contravention or an attempted contravention of the Migration Act. So that is broader. Similarly, there is a power to take copy or extracts of any document that is found on the ship or the vessel, so the purpose is a bit broader. Division 12A is drafted in identical terms to a similar set of provisions in the Customs Act and that is because—

CHAIR—That does not necessarily impress us at all, because what we are looking at here is the leapfrog or—as you call it, Senator Mason—the high watermark effect, where one standard is set there, so everyone thinks they can come up to it.

Mr Walker—It was done that way because they are powers that are exercised by enforcement officers at sea. We do not have any capacity for that. It is either the Customs maritime service or the Defence Force who rely on those powers in order for them to have procedures that would apply simply and uniformly, depending on the circumstances for the boarding, so they do not get caught with having to do slightly different things operationally if they are dealing with migration.

CHAIR—I think we can take it that it is a deliberate thing and not an aimless reflection.

Mr Walker—That is right.

CHAIR—I think the record will show that. I have a couple of questions about occupiers rights because Mr McMahon mentioned before about the noncooperation of a businessman, a restaurateur. Could you outline the rights and obligations of occupiers during a search and seizure operation?

Mr McMahon—I will have a shot at this and then I might hand it over to others. The act is expressed more in respect of our powers than the reciprocal rights. Consequently, when we serve a warrant there are some obligations that we place on ourselves under the act in terms of identifying who we are and providing them with the warrant, providing them with a copy et cetera. Where it goes from that point on depends a little on the level of cooperation that is provided. We do have the power to use reasonable force, for example. If someone locked the door in our face, we would have the power to use reasonable force, but then we have the test of reasonableness—you cannot knock down the front door if the back door was open. As a matter of policy—and I would imagine at common law as well—we have to operate in a way such that we do our business as expeditiously as possible and then leave. For example, it would be quite unlawful for us to stay longer simply because we thought this person was a bad person or whatever. We try to be in there for the minimum period of time, and there is a lot of planning about going in and withdrawing fairly rapidly after that.

Mr Walker—The power is specifically covered in subsection 251(8). It states:

An officer may use such reasonable force as is necessary for the exercise of his or her powers under this section.

That is very much the statutory basis for it.

CHAIR—Are there any penalties, for instance, for the occupier frustrating you, blocking you, misleading you, whatever?

Mr Walker—There is not anything specifically in the Migration Act in the sense of when you are executing the search. There are provisions relating to the harbouring of unlawful noncitizens. That is an offence under section 230 or 231. But that is cast more generally.

Senator MASON—Assault provisions apply if I try to stop an officer—is that right?

Mr Walker—That would be general criminal law.

Mr McMahan—We basically rely on the provisions of the Criminal Code. For example, it is an offence in the Criminal Code to mislead a Commonwealth officer. It would be an offence to impede a Commonwealth officer. Having said that, we take a fairly tolerant view on that. I cannot recall in the two years I have been doing this particular job that we have ever had cause to bring any charge against anyone. We certainly have been misled on a number of occasions. At one stage I asked officers to explore the potential of bringing charges against someone who lied about an unauthorised—

CHAIR—This is the life you chose when you joined Immigration!

Mr McMahan—I simply was going to get to the point that, in the end, it is not something that is likely to find its way into the courts. It is not going to have prosecution priority. There may well objectively be an offence but the chances of getting it progressed are slight.

Senator MASON—It has to get through the internal checks of your department and even if it gets through that the DPP has to approve it, so there are a few hurdles.

Mr McMahan—It is a DPP issue, yes.

Senator MASON—Mr McMahan, you flagged that you were aware of this committee's report dating from 2000—

Mr McMahan—Correct.

Senator MASON—and the government's response, which took a while. Did you say three years?

CHAIR—3½.

Senator MASON—In response to recommendation 7, the government recognised the merits of undertaking a review of existing entry and search provisions at agency level. You said that you have done that; that Immigration has embarked upon that.

Mr McMahon—That is correct.

Senator MASON—Okay. You passed that. In response to this committee's recommendation 12, the government accepted that recommendation in principle. The government accepted that Commonwealth agencies should adopt appropriate best practice training procedures and internal controls to ensure that the exercise of entry and search powers is as fair as possible. It says:

The Commonwealth DPP Search Warrants Manual is available free of charge to interested Commonwealth agencies.

Has Immigration adopted best practice training procedures, and how do you know they are?

Mr McMahon—The second question is the harder part of it. What we did as a result of the level of scrutiny and our own obligations under the act was go away and spend quite a bit of money to develop a course which took compliance officers right through from how you plan a compliance action to what is required for a valid warrant, how you would serve it and how you would retain it. That is a feature. We are continuing to build on that. We are spending probably a quarter of a million a year on training at the moment. Our objective is that at any one time 80 per cent of all compliance staff should have received training. It is a hard mark to achieve because no sooner have you trained somebody than they apply for a job in another part of the department and somebody else comes in. There is basically a two-stage module. There are around 290 compliance officers. Not all of them work in the field. About 90 of them have completed the entire course and something like 75 per cent have completed at least one of the modules. We have a very firm commitment to training.

Senator MASON—You are constantly reviewing that training?

Mr McMahon—We are. Our own discussions and external comment are fed into the training processes all the time. When something goes wrong we frequently put the test: how was this dealt with in the training package? We are about to revise this instruction again. It may have led to a different understanding from what we wanted to impart in the first place, between the instruction and the delivery of it, so we will go back and look at both the delivery of the training and the way in which the instruction expressed a particular thought.

Senator MASON—But is most of that scrutiny on the procedures internal scrutiny—the department reviewing its own procedures and outcomes?

Mr McMahon—Correct.

Senator MASON—You would not have any external ones, would you?

Mr McMahon—The only external ones have been a couple of complaints through the Ombudsman. I think we have had two in recent times. One basically found there was no defective administration and the other found that there was defective administration. The clearest message we are trying to send through the department in respect of it is that it is not enough for

someone to have formed a reasonable cause to believe; you have to actually demonstrate it and fully document it. I think in some cases people have relied at the time on a cluster of documents to form that view and all those documents may well have been before the decision maker at the time, but of course when you review it often the one document that comes out is the warrant which is on the register. So the message that we are getting out very strongly is that it must be a completely self-contained document.

CHAIR—You mentioned at the very start that the Ombudsman is doing a more general review rather than a case review. What is the timing of that and when do you think he will report to the department on his findings?

Mr McMahon—He is not doing a review. He has simply indicated that, for this year, he will focus on our warrant processes. So he has not said he is going to review it. I think the first stage of it was my meeting with the Deputy Ombudsman and some other senior staff. I think the first thing they wanted to establish was whether we were taking their comments seriously. I was able to convince them of that and I think they were reasonably impressed with the energy that we were putting into it, including trying to look at what we can do by the continuous process of self-assurance about our processes, and that is ongoing as well. We will be having a compliance conference in the next couple of months and a major agenda item will be warrants. I have been writing to the states, making sure that in each of the state offices there is a personal involvement of the state directors in respect of their scrutiny of their own processes and the application of the instructions.

CHAIR—There being no further questions, we thank you for attending today; we have appreciated your presence.

Proceedings suspended from 10.08 a.m. to 10.30 a.m.

PHELAN, Federal Agent Michael, National Manager, Border and International Network, Australian Federal Police

WHOWELL, Mr Peter, Manager, Legislation Program, Australian Federal Police

CHAIR—I welcome Federal Agent Michael Phelan and Mr Peter Whowell of the Australian Federal Police. Do either of you have some opening comments to make on your submission?

Federal Agent Phelan—Yes, I have a short statement to read out. Thank you for inviting the AFP to appear before the committee today. While the AFP obtains its powers of entry and search from a range of Commonwealth statutes, depending on the offence under investigation, it primarily exercises the powers available in the Crimes Act 1914. The government response to your previous report on entry, search and seizure provisions in Commonwealth legislation, which is the focus of this inquiry, clearly articulates the strict requirements the AFP must follow when exercising those powers. Our submission to this inquiry last year focused on the entry and search provisions in Commonwealth legislation created since your report in the year 2000, and on additional powers which the AFP believed its operational experience demonstrated a need for the government to consider the case for. I would like to take this opportunity to briefly update the committee on developments in the area of powers created since your report of 2000 before taking any questions you may have.

On search and seizure powers for the AFP Protective Services officers, the search and seizure powers under the Australian Protective Service Amendment Act, referred to in the AFP submission to the inquiry, have been replicated in the Australian Federal Police Act 1979, and took effect in July last year when the Australian Protective Service Act was repealed. Also in our submission we made reference to the Surveillance Devices Bill, and the committee would be aware that the Surveillance Devices Act 2004 received royal assent and commenced on 15 December last year. The Surveillance Devices Act 2004 implements the electronic surveillance model bill developed by the Commonwealth-state joint working group on cross-border investigations for the Commonwealth. It is part of a national scheme to provide consistent legislation across Australian jurisdictions. The act does not affect the existing system for telecommunications interception, regulated by the Telecommunications (Interception) Act. The act replaces the listening device provisions of the AFP act and Customs Act 1901 for the investigation of Commonwealth offences and state offences with a federal aspect. It retains them as part of the transitional provisions for the investigation of offences against the laws of the ACT. The act establishes a comprehensive regime for the use of optical surveillance devices, data surveillance devices, tracking devices and listening devices by the AFP, ACC and state and territory law enforcement agencies for the investigation of Commonwealth offences, and for the AFP and ACC in the investigation of state offences with a federal aspect.

CHAIR—Thank you. Our view of legislatures is that they have to approve changes to law. You would not have to be Einstein to say that in the last three or four years we have seen extension of powers for intelligence and law enforcement bodies, either as a reaction to events of increased threat of terrorism or to the advances in technology that the law always has to try to keep pace with and always trails behind. And, possibly, there is just a degree of incremental creep coming in. We have all these agencies with their increased powers, which we approve, but

we always wonder whether there is sufficient scrutiny of the exercise of those powers. I detect in most of the agencies, not unreasonably, just a bit of a reluctance to tick off on increased scrutiny, because no-one likes anyone looking over their shoulder. Has the AFP, more broadly, thought about this problem? Every time it seeks increased powers, does it ever look at how they will be scrutinised to make sure there is no abuse—other than saying, ‘Our internal procedures, discipline and ethos will guarantee it’? We know that is what it mostly does, but occasionally it does not. It is a very broad question.

Federal Agent Phelan—The best answer to that question is to look at the way the Australian Federal Police do it. We have been using search and entry powers for a long time—they are a bread and butter part of the law enforcement agency, with the purpose of gathering evidence. Over a long period of time we have developed some very stringent procedures and internal scrutiny where increased powers, particularly in the area of search, seizure and entry, are concerned.

To answer your question directly, there is a concurrent regime of scrutiny that applies to the increased powers that particularly the AFP has received since 11 September 2001. Our increased powers, particularly in the area of controlled operations and telephone intercept material, for example, are also scrutinised externally by the Commonwealth Ombudsman. The recent enactment of the surveillance devices legislation is also overseen by the Commonwealth Ombudsman’s office, requiring reports and so on. To that end, any of the new powers that have come in have also come under an existing regime of accountability and scrutiny, which the AFP works within and is quite comfortable to work within.

CHAIR—Are you convinced that the general ethos of your officers is that they are comfortable with scrutiny and it is not a burden placed upon them that they just have to bear?

Federal Agent Phelan—In terms of the external scrutiny, no. It is part and parcel of our business. At the end of the day, we are about accountability and prosecuting criminals and putting them before the court. So, for us, there is always that added judicial scrutiny when these instruments eventually appear before court, whether it be evidence obtained on search warrant, by telephone intercept or through the use of controlled operations. So, apart from internal scrutiny, there is always external scrutiny through organisations such as the Commonwealth Ombudsman.

There is ultimately judicial scrutiny of the way in which we have gone about our business. Procedural breaches occur there, and they have the potential to render evidence inadmissible. That, for us, is a very large risk—and we do not want to take that risk. In mitigation, when new pieces of legislation for the AFP are enacted, at exactly the same time we promulgate a set of internal guidelines to the whole of the organisation by our internal email system and place them on our internal hub or intra-web system. So each of the members are well and truly aware of their powers and their responsibilities in terms of accountability for those instruments.

CHAIR—We have been looking at one of the issues to do with technology—that is a warrant to seize electronic data which is fairly broad and so the whole hard drive is seized; you probably do not know in advance what is there. Some information may be relevant to the warrant but much of it may not be, which raises the question of how that information is protected properly. That is the first part. Secondly, is there any way of restricting warrants further back?

We can give an example, because it has already been put down in the parliament. It has the added complication of parliamentary privilege, so you do not need to concern yourself with that. A hard drive was seized and there were thousands and thousands of documents, and we had to determine whether these documents were covered by privilege. Just to save time and money for everyone, we also got the QC we employed to see whether they were within the warrant or not. As it turned out, not one document was within the warrant. That is only an example, but I wonder how often this is happening—that a warrant is given to seize electronic data and 100 per cent or 99 per cent of the massive amount of data is not relevant to the warrant—and what we can do about it.

Federal Agent Phelan—To put that in perspective, a number of options are available to us. When you go into premises with a validly issued search warrant and find a computer, for example, that warrant gives you the authority to see what is on it—in the first instance, to find out whether or not there is any relevant material. If there is relevant material and it falls within the scope of the warrant, we will seize the hard disk and take it back. If we get to premises and have the authority under the warrant to seize a hard disk but cannot see what is there because it has security encryption or the like whereby we cannot get into it at that time, we take the hard disk away and image it, as a matter of practice, and then look to see what is there. Obviously we do not want any material that is on there that is not relevant to the warrant. For written documents, as you would appreciate, if they are out of files and have no probative or evidentiary value, we return them. When it comes to electronic equipment, that becomes a little problematic.

At the moment, what we do is extract the material that is relevant. We have to look at everything to see if it is relevant and falls within the scope of the warrant, and extract the material that we require—that is what is given in evidence. But the actual hard disk itself is kept, because it is the hard disk that is the primary evidence. It is difficult, as you could appreciate, to give the hard disk back, because if we had to go to a court of competent jurisdiction they may ask, ‘Where is your primary document?’ The primary document is the hard disk.

CHAIR—My next question is purely voyeuristic; I do not know if it is relevant to our inquiry. If you find other information there, not relevant to the warrant but of a criminal nature, does that entitle you to seek a new warrant to seize that material?

Federal Agent Phelan—Generally speaking, under the general provisions, if something is within the scope of the warrant in the first place—if you are there lawfully and you find something else in relation to another criminal activity—you can seize that material anyway under the existing provisions of the warrant. That would be fine. You would not have to seek an additional warrant. You cannot get a search warrant to search the Australian Federal Police premises. Remember, the search warrant is to actually enter and search the premises to obtain the evidence. We already have possession of the evidence, so getting a warrant to enter is not necessary at all.

CHAIR—You mentioned in your introduction that the stored communications surveillance devices legislation went through and was given royal assent in December. Have those sorts of powers been used this year by the AFP, and how is it performing as a piece of legislation to assist you?

Federal Agent Phelan—It is performing well. I could take on notice exactly how many times we have used the legislation.

CHAIR—No, I do not want to know.

Federal Agent Phelan—It is working well, particularly the provisions that require senior executive officers to be able to authorise the placing of a tracking device, for example, where there is no intrusion onto property or into vehicles. That seems to be working well, as well as getting judicial warrants for intrusion into premises or vehicles. Of course, we have not yet had our first report on that to parliament.

CHAIR—No.

Federal Agent Phelan—I do not know off the top of my head, but they might be every 12 months.

Mr Whowell—I think they are.

Federal Agent Phelan—Normally they are every 12 months. With controlled operations they are certainly once every 12 months, so I would imagine it would be in the same cycle but I am not quite sure.

CHAIR—I think prior to that the Cybercrime Act was passed. Are you aware of any difficulty in executing warrants or otherwise exercising powers under that act?

Federal Agent Phelan—Certainly there were initial problems with accessing stored communications. You would go onto the premises and use the person's broadband get into their accounts, but now it gives us the ability to access information that is there but not stored; what they have got access to but not what is on the ISP. We would need a separate warrant to be able to go and do that. We have not had any problems with that so far.

CHAIR—So have occupiers raised objections?

Federal Agent Phelan—Not that I am aware of.

CHAIR—Can we move on to the protocols covering the execution of search warrants and the seizure of material. What practices or procedures exist to support the execution of search warrants and associated seizure provisions? All we are talking about is guidelines, manuals, codes of conduct or agency procedures.

Federal Agent Phelan—Of course there is the Director of Public Prosecutions search warrant manual that we would use to assist us to draft and that also has general provisions in relation to the law on search warrants. Internally, we have guidelines and policies that are promulgated throughout the whole of the organisation, that are accessible to everybody and that dictate levels of safety for search warrants, what we are to do with the property, how it is to be stored, how it is to be recorded and all those sorts of things to maintain the chain of custody and the continuity of that evidence, to preserve that evidence and also to protect the rights of the individual. That

includes that, once material is seized pursuant to a warrant, if it is not relevant it goes automatically back to the person who owns the material.

CHAIR—What sort of indication do you give to an occupier who a warrant is issued against as to their rights?

Federal Agent Phelan—With every search warrant there is a requirement under the act for us to give them their set of rights under the act and exactly what is available to them in terms of what they are able to get—a receipt for the property. There are a number of provisions contained within the Crimes Act and we actually give the occupier a written notice as to exactly what their entitlements are under the act.

CHAIR—Are the various procedures and manuals publicly available or are they an internal working document?

Federal Agent Phelan—They are an internal document and, essentially, they are evolving documents as well. So as new circumstances dictate, as technology moves on, as the legislation changes, we are continually updating those documents.

Senator MASON—What are your benchmarks for best practice?

Federal Agent Phelan—I suppose the benchmark for best practice is the legislation itself; that is what we base it on as the highest point. Then in terms of best practice, there is the judicial scrutiny that comes from the search warrants and what would come out of cases where search warrants have been executed and they have had some sort of scrutiny before the courts. If the court makes comments, for example, what we learn as a result gets moved into the guidelines.

Senator MASON—External scrutiny—that is the court’s internal scrutiny, obviously, within the AFP itself?

Federal Agent Phelan—Within the AFP.

Senator MASON—Do you at any stage compare how you operate in this context with overseas agencies? Is that done, or is that voyeuristic as well?

Federal Agent Phelan—Not as a matter of course. We are quite happy with the procedures we have.

Senator MASON—I was just wondering.

Federal Agent Phelan—In my experience—and I have worked overseas myself—at the end of the day I think we have a very good regime here. It is not only a very good guideline regime that talks about the regulatory functions but it also brings in those other aspects like the safety of the officers, the safety of the premises and things like that. Here we are talking about search warrants for things like drugs with clandestine laboratories and precursor chemicals and all those sorts of things. A search warrant on a bank is totally different from a search warrant on a clandestine laboratory, and the guidelines cover the full gamut of what we need to take into account when exercising the police powers that are available to us.

The extra level of scrutiny that we have always is the internal investigations regime of the AFP of complaints under the Australian Federal Police Act, which of course means that any member of the public can complain about police conduct on any matter whatsoever. Every complaint under that act has the scrutiny of the Commonwealth Ombudsman as well. Quite often, if it involves search and seizure, the Commonwealth Ombudsman will pass comment in relation to those procedures and that comes back to us and, if necessary, we will alter the guidelines accordingly. So these things are not written in stone.

Senator MASON—And you report to parliament ultimately as well, I suppose, so there is parliamentary scrutiny of a sort.

Federal Agent Phelan—Absolutely.

CHAIR—You also have to assist some other agencies with their search and seizure powers which are not always identical in procedure to yours. Do you have to go and learn their procedures before you assist them in some of these circumstances?

Federal Agent Phelan—If we are executing warrants on their behalf under the Crimes Act 1914, we will follow our procedures to do that because effectively we are the ones executing the search warrants on their behalf. We do not abrogate our reporting responsibilities or internal guidelines for that. The only thing that is a little bit different is that on occasion, if they request it, the actual evidence that is seized is handed to the agency upon whose behalf we are acting for them to look after basically as de facto custody for us, because they have to do their investigation if it is not for us. For example, the Health Insurance Commission may be doing an investigation that the AFP is not but we will exercise the powers on their behalf, seize the material according to our procedures and policies and then hand the material to them. Then when it comes back we acquit it through our own register system.

CHAIR—I think in your document of a year ago you only make two more territorial demands. One is delayed notification search warrants and the other is notices to produce. Would you like to explain to the committee what your view is on those and explain to us what your aims are?

Federal Agent Phelan—Perhaps, first of all, in relation to notices to produce, because I think that is a little less complex, as I alluded to earlier on, the gambit for which we get search warrants can be wide-ranging, all the way from hard entry search warrants on premises where people have firearms to what we would call friendly warrants on, say, financial institutions and utilities—Telstra and so on—where we can obtain information. Those utility type agencies want some sort of judicial authority to be able to hand the material over so they have protected themselves primarily from privacy provisions and also, indeed, I suppose, civil action, if that were ever contemplated by the person mentioned in the material.

It has been my experience over nearly 20 years in this organisation that the only reason we have to get those types of warrants—the ones we call friendly warrants—is because they require it to cover themselves against those types of civil actions. It is not as if they do not want to hand over the material. The amount of time it takes to put together search warrants and so on can sometimes be detrimental to an investigation. When you are putting together a search warrant you need to satisfy the magistrate fully. You cannot just do enough to satisfy them to give you

the warrant; you have to give them all of the material. That can indeed take a long time to put together and it can be very long and laborious to read.

However, when these things can be done internally—and we would advocate that only the commissioner delegating that power down to, say, a senior executive officer at the rank of commander or above should be able to issue those notices to produce—then the banks, financial institutions and utilities would be more than happy to comply with that, and we do not have to go through a very onerous regime to be able to obtain that information. Similar provisions exist within the Proceeds of Crime Act 2002 where we obtain that information from financial institutions—

CHAIR—That does not help here—leapfrogging does not help.

Federal Agent Phelan—Yes, I understand.

CHAIR—Pointing to where it exists somewhere else does not help. Just on that point—and it is a reasonable case you make—do you have statistics on how many friendly warrants you seek a year? Do you have statistics on whether you have any rejection rate? Before you come forward with this proposal I am sure it would be enhanced if you could say, ‘We put in for 400 friendly warrants, as we define it, and they were all granted’ rather than saying that 60 were not. Then we would want to know why those 60 were not granted when they would be automatically done on a notice to proceed or produce.

Federal Agent Phelan—I understand that. I may be able to get that material. It might be very hard to extract.

CHAIR—It may be hard—I can see that. Now I am asking for your overall impression, which we will not hold you to if the statistics are at variance.

Federal Agent Phelan—My overall impression is that extremely few friendly warrants would have been knocked back by magistrates who issue those warrants. I would say it would be a very small percentage that has been knocked back. I would also say that, in most investigations we would do, the majority of search warrants in those major investigations would involve friendly warrants. Of all of the investigations that we would do, there would normally be only a couple of hard warrants, for want of a better word, for when you are going into target premises to actually gather evidence, normally at the culmination of an investigation. But, throughout the investigation, there is cause to obtain material along the way a lot more times than in that one search.

CHAIR—So, if they were erroneously executed, you would not mind that the person adversely affected gets compensation, I suppose—that is, for those that are rejected or where there are flawed processes in the notice to produce?

Federal Agent Phelan—We would also say that the senior executive officers of the AFP issuing those notices to produce would also look at those notices themselves and may knock them back. We can look at a regime that is similar, which is where we have authority to do controlled operations. Senior executive officers have rejected applications for controlled

operations put forward by members of the organisation based on insufficient evidence, and they are reported in the annual report. So it is not ‘tick and flick’ by any means.

CHAIR—That is good. What about delayed notification search warrants? You indicated that there is a slightly tougher issue.

Federal Agent Phelan—It is a bit tougher. In the regime that exists at the moment, we have to notify an occupier of a search warrant and it can potentially hinder ongoing investigations. I think in our submission we highlighted the situation of a planned terrorism act, for example. We may not have enough evidence to actually charge somebody, but we know something might be on the premises—there may be a map of a target that might be blown up or of something they will do some sort of terrorist act to. We might want to get in there, look and see what is in there and what they are actually planning. Then we might want to be able to monitor them, continue the investigation further down the track to see what is going on and actually gather enough evidence on either the whole conspiracy or other players that we do not otherwise involve. If we go in there to find out what is in there, under the current legislation we have to let someone know that we were there.

CHAIR—So this is to gather evidence rather than intelligence? There is quite a difference.

Federal Agent Phelan—That is right. At the end of the day if we know there is a map, that is evidence. Ultimately it will be evidence but we would say that we would not want to seize it at that point in time. We might want to take photographs of it but we would not want to alert them that we were on to them. That is just one example on the terrorism front. There are other examples particularly to do with narcotics or something like that, because it is not always that the Australian Federal Police have control of the substance. If, for example, illicit drugs were not detected at the barrier but through our own information through informants and we have identified that it is at a certain location, it is sometimes extremely handy to know exactly what we are dealing with, how much, where it is and all those sorts of things. We can get that by entering the premises but not necessarily seizing it—although indeed we could seize it and substitute it, for example—while not alerting the occupiers of the premises that we are on to their importation or criminal venture, because there may be other players in the venture that have not yet come to light for us who will not come to light until later on down the track through electronic surveillance or physical surveillance or even some foot-slogging detective work through documentation and so on. So there are occasions when actually letting people know we are doing search warrants will affect the investigation, so as a matter of course we do not do search warrants for that purpose because we could be potentially jeopardising our own investigations. The fact that we are not doing search warrants on these places when we perhaps should be can indeed sometimes lose us evidence or valuable information that may flow from the evidence that we know is on the premises. So it does put us in a situation that if we had that authority—and we would want scrutiny of that afterwards; that would be no problem—in that way we could at least delay the notifications to the occupiers until such time as it would be operationally safe to be able to do so, not that we would never do it.

Senator MASON—Chair, I do not have any questions except to reiterate the general concern reflected in your opening question—and you really put this very well—that, over at least the last 10 years with technology, the threat of terrorism and incrementalism, this committee—and I suspect the Senate, and the parliament as a whole—is concerned that agencies of the executive

be held to account. That is the nub of it. All the evidence before us, including the evidence earlier today, reflects that concern. We have to be sure that agencies are held to account and that there are measures to hold them to account.

CHAIR—It is really a two-edged sword, though. It is not that there is a lack of trust. I find that when you put in accountability mechanisms the behaviour rises to meet the accountability mechanisms, so the accountability mechanisms are not necessarily there to run witch-hunts against anyone. We know for a fact that an intensive Senate estimates committee process means public servants—as they have told me—think twice about doing something, because that particular body may bring them to account one day. That is the point we are making. For every action there will be a reaction and provided it is in balance it should be good. Thank you, witnesses, for coming today. We appreciate your evidence.

[11.00 a.m.]

GRANT, Mrs Marion Estelle, National Director, Border Compliance and Enforcement Division, Australian Customs Service

JANECZKO, Mr Richard, National Manager, Investigations, Australian Customs Service

WHITEHOUSE, Ms Anna Kirstin, Senior Government Solicitor, Australian Government Solicitor

CHAIR—Welcome to today's proceedings. I think you know the rules applying to giving evidence.

Ms Whitehouse—I think I need, first of all, to point out that I am the senior government solicitor at Customs but I actually work for the Australian Government Solicitor. We are their in-house legal service providers. I am just here to give technical legal—

CHAIR—Absolutely.

Ms Whitehouse—Is that okay?

CHAIR—Yes. Welcome to the majors. You are aware of the rules, I think, applying to the giving of evidence before the committee. Whatever evidence you give will be covered by parliamentary privilege. Would one of you like to make an opening statement?

Mrs Grant—Customs does not have an opening statement this morning. We rely on the submission that we have presented to the committee and we are happy to take the questions you may have for us.

CHAIR—Very good. The agency's submission refers to self-imposed procedural safeguards which help ensure that the legislation is administered in a fair way. Of course you have given the example of the *Australian Customs Service Manual*, volume 18. Our first question is: what is the authority for these procedures and documents?

Mrs Grant—The authority for volume 18 in particular?

CHAIR—Yes, on what authority does it rely, legislative or otherwise?

Mrs Grant—Customs has a series of manuals that cover the range of our operational business and we use those manuals really as a way of describing to officers the legislation under which they are working, any policies and procedures that Customs has developed that spring from the legislation. The manuals would have the status of an internal document guiding the actions of our officers but very much reflecting what the legislation requires as we go about our duties. So the manuals themselves have no particular legal basis. The contents are updated every time the legislation might be amended. We will then reflect any flow-ons into those manuals as a result of revised legislation.

Ms Whitehouse—They are underpinned by a number of provisions in the Customs Act regarding search and seizure powers, the power to seek warrants to search and to seize material on premises, conveyances et cetera. Customs also has the power to seize particular goods without warrant in Customs places, which is effectively the airport. That is limited to goods listed in the prohibited import regulations—quite a narrow power. They are the key powers that Customs operates under.

CHAIR—Do you have separate guidelines for the execution of Crimes Act warrants?

Mrs Grant—Customs as an agency is not able to execute Crimes Act warrants. When we need to undertake an investigation involving that type of warrant, we call on the AFP to execute the warrants on our behalf.

CHAIR—Are any of these documents we are talking about publicly available documents that can be scrutinised, or are they like Immigration’s internal working documents?

Mrs Grant—The Customs manuals have traditionally run on a set of confidential versions and public versions. There are a number of volumes. The investigation manual I believe is a confidential version with no public version available.

Mr Janeczko—That is right.

CHAIR—How much information are you required to give to, let us say, what we call ‘occupiers’? What sort of information are you required to give before you execute a warrant or are in the process of executing a warrant against them?

Mr Janeczko—If you want the legal answer, Marion will give it to you.

CHAIR—I want the practical one.

Mr Janeczko—We identify ourselves and we introduce ourselves and let people know what their rights are and why we are there—the normal sort of procedure. We also have a format where we talk to people as we leave to see whether or not they have any complaints. We go through a process like that and we prepare ourselves with a pre-warrant report, which goes through our manager, and a post-warrant report, and in that officers record the fact that they have been through this process of identifying people and then recording any comments that might be made by the occupier or any occupational health and safety or other issues.

CHAIR—Is there anything to add legally, or has he covered it?

Ms Whitehouse—There are specific provisions which provide that the occupier is entitled to be present during the search warrant et cetera.

CHAIR—I think it is the general view of Customs that you would rather there not be an overarching set of government protocols. In what way is Customs different in that it really needs its own set rather than an overarching set of government principles with regard to entry, search and seizure?

Mrs Grant—Customs is not different, and Customs does follow the overall Commonwealth guidelines for prosecution. You might be picking up a reference somewhere in this document to a particular question in the terms of reference about protocols.

CHAIR—It is really to do with seizure more than anything else. By the way, there may be a very good reason here. We are just trying to take evidence to see what it is.

Ms Whitehouse—The seizure provisions in the Customs Act for the most part correspond with the equivalent provisions in the Crimes Act.

Senator MASON—Are there any special concerns that you have?

Ms Whitehouse—What is quite specific to Customs is this ability to seize particular goods in the absence of first applying for a warrant. The most common scenario would be where narcotics are found at the airport, for example. Clearly, there is a need to seize those goods at the time rather than have to rely on the AFP because of the timelag et cetera.

CHAIR—Apart from at airports, can you seize goods without a warrant?

Ms Whitehouse—Only narcotics.

Mrs Grant—Also in other Customs places—

CHAIR—Yes, I assumed that.

Mrs Grant—apart from an airport, if there are special forfeited goods—basically anything that is a prohibited import or export—we can seize goods without a warrant. In any other case we must get the warrant before we can seize.

Senator MASON—In this committee's 2000 report on search and seizure, recommendation 7 was accepted in part by the government. The government accepted the merit of undertaking a review of existing entry and search provisions at agency level. Has that been done by Customs since 2000?

Mr Janeczko—We are constantly looking at our legislation. I am not sure if that is the question.

Senator MASON—I suppose it is partly, but I think what the government was getting at here was that agencies should be taking a specific review of existing entry and search provisions. Immigration said that they had completed one.

Mr Janeczko—What was the recommendation number again?

Senator MASON—Seven.

Mrs Grant—Customs has not undertaken a specific review following that recommendation. The Customs search and seizure provisions were significantly overhauled a couple of years prior

to that when we had a major rewrite of the Customs Act to modernise our search and seizure provisions to bring them in line with general Commonwealth requirements.

CHAIR—Probably with the exception of the Federal Police and the department of immigration, search and seizure is your core business more than it is for all the rest of the government departments, isn't it?

Mrs Grant—Yes, especially when search and seizure provisions are in the Customs Act, we have our own Customs prosecutions and we do all of our own investigations, apart from narcotic matters which are handed over to the AFP.

CHAIR—Have you had a chance to look at submission No. 8 from the Law Council of Australia, the business law section?

Mrs Grant—Yes, we have.

CHAIR—They make what borders on a complaint, I suppose, and suggest that warrants are being used by the Customs Service as a first resort rather than a last resort, and they say that is despite undertakings that may have been given upon the introduction of the trade modernisation legislation. They are critical of the exercise of covert searches, and specifically of covert examination of cargo passing through the container examination facilities. I am not endorsing this at all; I am giving you the chance to respond if you would like to.

Mrs Grant—When we had a look at that submission we formed the view that there might be three different things being confused here: our audit monitoring powers as opposed to search and seizure provisions in relation to an investigation, the fact that we are examining a significant amount of cargo through our container examination facilities and the fact there are no warrants involved in requiring containers to go through those facilities. So it was a little bit difficult to work our way through some of the information that had been provided.

CHAIR—We might turn to our lawyer to tell us what the Law Council was on about.

Senator MASON—I wish I knew. I want to ask a question to do with practice. The government reply to recommendation 12 of this committee's report was that the government accepts that Commonwealth agencies should adopt appropriate best practice training procedures and internal controls to ensure that the exercise of entry and search powers is as fair as possible. Do you believe that you have adopted best practice training procedures? Have you reviewed your training procedures in light of that—particularly if, as you say, your power has changed enormously? Did you review training procedures as a consequence of that?

Mrs Grant—Customs certainly overhauled all of its training. For our investigation function we have what we call our QCIC—qualifying customs investigation course—which is to the certificate IV standard. We work closely with the AFP and in fact it is delivered through the AFP at their college. So we train our investigators to that same level. That is the face-to-face training. It is preceded by quite a significant amount of online pre-course qualification before you are allowed to actually go to the face-to-face training. During the 12 months following, the training is followed up with an on-the-job assessment of the competencies before people are actually

issued with their certificate to say that they are now a qualified investigator. We have a fairly rigorous training program in place for that aspect of our business.

The other aspect that the Law Council touched on was the monitoring powers, which relate to our audit activity. People have to be trained before they are authorised to have monitoring powers issued to them. With all those audit powers, we do the activities with the consent of the occupier of the premise that we would be going to. If they choose not to give us consent or withdraw consent in writing at any time during the audit after they had previously given consent, we then need to seek a monitoring warrant if we are to complete that audit without consent.

Senator MASON—Do you have any external review of those training procedures? I suspect it is probably like the AFP. There would be judicial comment upon searches that were done which were either illegal or poor. What scrutiny would you have? You would have internal scrutiny, I suppose, and judicial scrutiny. There is parliamentary scrutiny. What sort of scrutiny is there?

Mrs Grant—I was listening to the comments that our colleagues from the AFP were providing and thinking we would have to provide a very similar answer to you if you asked us that question. There are all of those external scrutinies. We also run a quality assurance program, which is the AFP's quality assurance for cases. After a case we will assess every element of the case file to see how it was done, whether it was done in accordance with protocols, whether it could have been done better and what lessons needed to be learnt from that particular case.

CHAIR—So if I am a Sydney business identity and I believe that I have been done over by Customs in the execution of a warrant what remedies are available to me that I could take up?

Mrs Grant—In the first instance, you could lodge a complaint with Customs. We have a formal complaints and compliments system that has standards for dealing with complaints. There is the external scrutiny by the Ombudsman and there are ministerial representations—the usual range of places people can record their complaints.

CHAIR—The Ombudsman would be the main port of call, one would imagine, outside your internal complaints process?

Mrs Grant—Yes. We have not had a complaint about a warrant to the Ombudsman for a considerable period of time. I just cannot recall one in recent years.

CHAIR—Congratulations. Thank you very much for coming today and assisting us with our inquiry.

[11.16 a.m.]

MACAULAY, Ms Louise Anne, Director, Enforcement Policy and Practice, Australian Securities and Investments Commission

CHAIR—Welcome. Ms Macaulay, I think you know the procedures in giving evidence before a Senate committee. Would you like to make an opening statement?

Ms Macaulay—Just a very short one. Thank you for the opportunity for ASIC to appear at this hearing. We are acutely aware in our day-to-day business that the exercise of our powers does intrude on common law rights, on people's personal rights, and so we welcome the opportunity to appear at these sorts of Senate hearings. We see this as a vital part of the scrutiny that we are subject to. That allows us to be able to exercise these powers confident in the knowledge that, if we exercise them properly, we are doing so in accordance with properly scrutinised government policy.

The only other thing I have to add to our submission is that, since we put it in, the Telecommunications (Interception) Amendment (Stored Communications) Act 2004 has come into force. We supported the introduction of that legislation. It clarified the position in relation to access to emails and other forms of stored electronic communication. That is a form of communication that we access quite often, because of the type of people that we regulate. A lot of business is done using those forms of stored communication, and without the ability to access that material we are stymied in our regulatory objectives.

CHAIR—Have you a slightly different problem from all the other agencies that have appeared before us? The clients or customers which you are dealing with are more likely to be litigiously orientated and much more likely to have the funds to pursue it.

Ms Macaulay—Yes, I think that is certainly the case. If you look at recent decisions in relation to search warrants, you will see that a number of them have involved ASIC search warrants. There was one that involved an ATO search warrant. That is okay. We are happy to have judicial review of the exercise of our powers. Sometimes we might question the purpose of engaging in that litigation. But that is not an issue, I do not think, for this committee.

CHAIR—One of the problems which we have been wrestling with is the increased powers given to agencies such as yours. You have the right to have a warrant for electronic data. But, given the nature of where electronic data is stored, we often find that only one per cent of the total amount seized is relevant to the warrant. You cannot know that in advance. How do you deal with that? How do you protect the privacy?

Ms Macaulay—You are right. We have had a couple of recent situations where that has been an issue. There is a judgment of Justice Branson in relation to Mr Kennedy's application. We seized some material from his premises. There is also the Harts case, which we have had a look at. We think those decisions have been useful because they have clarified the operation of those cybercrime provisions of the Crimes Act, both for us and for the community that we regulate.

We have also now had experience in using a number of these search warrants where we are able to seize computer material and we make a decision at the premises that we need to copy the hard disk. We have now been through a number of those situations, so we are starting to develop some protocols as to how we deal with that.

CHAIR—I do not think we need a recitation of how the law works as applied to your organisation, but quite often what is crucial is what underlies it in terms of manuals and procedures et cetera. Could you give us a brief indication of how you operate at that level.

Ms Macaulay—Certainly. There are two powers which allow us to enter premises and seize material: Crimes Act provisions; and we have some provisions in the ASIC Act, which only come into effect if we have served a notice to produce documents and nothing has been produced or we believe that not everything has been produced. By far the bulk of the search warrants we execute are Crimes Act search warrants. We follow the DPP search warrants manual in relation to that.

Senator MASON—Do you execute them?

Ms Macaulay—No, the AFP executes them on behalf of us. So we follow AFP procedures. We use the guidelines that the AFP agreed with the Law Council of Australia in relation to privileged material. We always seek the advice of the DPP before we execute the warrants. We provide written information to the owner or the occupiers in accordance with all of the DPP procedures. We allow the occupier to review the material before we remove it. We issue a receipt. The material first goes to the AFP premises and then they are empowered under the Crimes Act to release it to us. We keep all the material in secured workrooms, either in a central secured document collection point or in secured workrooms. We have a litigation support system where we record the documents and the search warrant. Very often we just work with electronic copies of documents and keep the originals secured. We have got a manual and a policy on handling this sort of material. We have also got a general ASIC policy on handling sensitive information. We have obligations under section 127 of the ASIC Act to keep confidential any confidential material that we obtain in the course of exercising our compulsory powers.

CHAIR—So you have not been in known breach of that?

Ms Macaulay—No, no breach that I am aware of. We handle a lot of very sensitive information. You can imagine that we receive large volumes of documents when we carry out our investigations. It is really our bread and butter work in investigations, having procedures and processes in place to deal with this information. We are constantly dealing with issues of commercial confidentiality as well as simply the confidentiality that exists or the need to secure documents that we have seized and also issues like legal professional privilege or privilege against self-incrimination. Of course, search warrants are not the only way we obtain material; we have got power to issue notices to require people to produce material. By far the bulk of the material we receive is from notices, but the same principles apply.

CHAIR—Those notices go to third parties rather than to the target usually, do they?

Ms Macaulay—They can go to any person, so they can in fact go to the target. We only use search warrants where we have an apprehension that the evidential material will leave the premises, may disappear—

CHAIR—Will be destroyed.

Ms Macaulay—I have got some statistics. They relate to matters which are still on foot. The number of search warrants that the AFP executed on our behalf in 2004 was 44. That is for matters which are still on foot, and I suspect that most of the matters—

Senator MASON—That is warrants?

Ms Macaulay—Warrants, sorry. Most of the matters would still be on foot.

CHAIR—Can you compare that with notices to produce?

Ms Macaulay—Yes, thousands of notices. That is just not in the context of our investigation, because we also use notices in our surveillances where we are looking at our regulated entities just to check their compliance.

Senator MASON—Do you execute the notices?

Ms Macaulay—We issue the notices, yes.

Senator MASON—The AFP or you?

Ms Macaulay—We do. We have got quite extensive powers within the ASIC Act to issue notices and have people produce material. We can also have people attend our offices and answer questions on oath in a private examination. We are used to using these powers; we use them a lot and we use them against people who are very well informed, very well resourced and who have a lot at risk in terms of reputation. Whilst much of what we do does not necessarily involve criminal behaviour, it does involve significant serious misconduct.

CHAIR—When the relevant target has complaints to make about the execution of the warrant and its nature, I assume that the options available for a complainant are fairly similar to those of the other agencies, but you might like to indicate to the committee what they are.

Ms Macaulay—If they think there has been an illegality, they are able to approach the Federal Court and seek an ADJR review of it. Further down the track, if we seek to rely on some of this material as evidence, they can challenge its admissibility during the course of a prosecution. They can make a complaint about the conduct of our officers, and we have internal procedures that deal with that. I have a professional standards manager within my area who deals with these complaints. If we think there has been any criminal conduct involved, we would refer that complaint to the AFP. The Ombudsman is also available to look at these complaints.

CHAIR—I think that is fairly common with the agencies that we have been discussing.

Senator MASON—I am happy with your questions, Chair.

CHAIR—I think we have got to where we needed to go. Thank you for your attendance this morning; we appreciate it.

Ms Macaulay—My pleasure.

Committee adjourned at 11.26 a.m.