COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE

Reference: Surveillance Devices Bill 2004

MONDAY, 10 MAY 2004

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

WITNESSES

SENATE

LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE

Monday, 10 May 2004

Members: Senator Payne *(Chair)*, Senator Bolkus *(Deputy Chair)*, Senators Greig, Ludwig, Mason and Scullion

Participating members: Senators Abetz, Bishop, Brandis, Brown, Carr, Chapman, Eggleston, Chris Evans, Faulkner, Ferguson, Ferris, Harradine, Harris, Humphries, Kirk, Knowles, Lees, Lightfoot, Mackay, McGauran, McLucas, Murphy, Nettle, Robert Ray, Sherry, Stephens, Stott Despoja, Tchen, Tierney and Watson

Senators in attendance: Senators Ludwig, Mason, Payne and Scullion

Terms of reference for the inquiry:

Surveillance Devices Bill 2004.

Committee met at 9.31 a.m.

CHAIR—This is the hearing of the Senate Legal and Constitutional Legislation Committee's inquiry into the provisions of the Surveillance Devices Bill 2004. The inquiry was referred to the committee by the Senate on 31 March 2003 for report by 27 May 2004. The bill proposes to consolidate the regulation and use of surveillance devices, to provide a framework for cross-border consistency of use of the devices and to include a reporting system for use of the devices in most circumstances. The committee has received five submissions for the inquiry, all of which have been authorised for publication and are available on the committee's web site.

Witnesses are reminded of the notes they have received relating to parliamentary privilege and the protection of official witnesses. Further copies of those notes are available from the secretariat. Witnesses are also reminded that the giving of false or misleading evidence to the committee may constitute a contempt of the Senate. The committee prefers all evidence to be given in public but, under the Senate's resolutions, witnesses do have the right to request to be heard in private session. It is important that witnesses give the committee notice if they intend to ask to give evidence in camera.

[9.32 a.m.]

DARGAN, Mr Brian, Manager Law Reform and Commercial Legal, Australian Crime Commission

TEBBET, Mr Robert John, National Manager, Technical and Physical Surveillance, Australian Crime Commission

TINKER, Mr Raymond, Head of Investigation South East Asia Organised Crime, Australian Crime Commission

CHAIR—Welcome. I invite you to make a short opening statement, and at the conclusion of that we will go to questions from members of the committee.

Mr Dargan—The Australian Crime Commission commenced operations on 1 January 2003. It was formed through the amalgamation of the former National Crime Authority, the Australian Bureau of Criminal Intelligence and the Office of Strategic Crime Assessments. Part of the role of the ACC is to conduct intelligence operations and investigations into serious and organised crime. Such operations and investigations must first be approved by the ACC board, which consists of the heads of all Australian police services, the heads of Customs, ASIC, ASIO and the Secretary of the Attorney-General's Department. The board has so far approved operations and investigations into several main areas of serious criminality. Those areas include firearms trafficking, money laundering, tax fraud, established criminal networks, vehicle rebirthing, identity crime, amphetamines and related substances and South-East Asian organised crime.

In relation to each board determination a head is appointed by the CEO. The head is responsible for all operations and investigations on each determination. As investigative activity occurs across Australia there is a team leader in each ACC office who conducts investigative activity in that jurisdiction and reports to the investigation head. Each investigative team may be staffed by investigators, financial analysts, a lawyer and administrative staff. Mainly each of the ACC determination investigations relate to serious indictable offences being planned or accomplished by organised crime figures and groups. The types of offences investigated range from narcotics, firearms trafficking and crimes related to organised racketeering through to the laundering of organised crime profits.

In all investigations, electronic surveillance devices can play a critical role. At present, investigators need to observe the legal requirements for the use of devices, which vary between jurisdictions. A single uniform system would be of great benefit. Last year the ACC obtained around 174 warrants for listening devices. Currently, material gathered from listening devices is secured, recorded and stored by internal exhibit registrars in each ACC office. It is envisaged that all recordkeeping required by the bill will be centralised in Sydney. This is similar to the approach we have taken under other Commonwealth legislation, such as TI, controlled operations and assumed identities. It will support compliance with the recordkeeping and reporting requirements of the bill and assist ombudsmen inspections.

CHAIR—Thank you very much. Mr Tebbet and Mr Tinker, do you wish to add anything at this point?

Mr Tebbet—No.

Mr Tinker—No.

Senator LUDWIG—With regard to emergency warrants, could you give me some examples of when the ACC would require the use of that power?

Mr Tinker—I will lead off. Once commenced, the investigations conducted by the ACC often require a mix of, in the first instance, perhaps 60 to 70 per cent of resource issue in the surveillance arena. That is physical surveillance in the main. Going along with that is electronic surveillance. The road to targeting organised crime figures in the first instance largely involves physical and electronic surveillance. The final stages of an investigation involve issues that can take over from that surveillance activity, once plans and orders become overt and the offences are likely to be committed immediately or, in fact, have been committed and sufficient evidence has been gained through the use of tools such as surveillance and electronic surveillance. Once that decision is made, the mix of investigative resources changes and the use of surveillance and electronic surveillance falls off.

Senator LUDWIG—That is helpful, but it does not help me to understand why there is a mix of tools available to you, which include telecommunications interception warrants and the like. They all require warrants. We have a bill that is seeking to use certain technologies in particular ways for covert surveillance, as I understand it, without a warrant. In other words, there would not be the rigour that you would normally go through in determining that a warrant has to be put before a judicial officer. I was trying to ascertain when you would require the use of such a power, which is different from that which you can use for telecommunications interception, where a warrant is required. I am trying to understand why you want that power in the first place. Why is it necessary? Why can't you get a warrant?

Mr Tinker—Since 1979, that power has been available to investigative authorities through the listening device provisions of the Customs Act. The test for when the commencement of that activity occurs is based on reasonable suspicion that a crime has been committed, will be committed or is likely to be committed. That test is very similar in nature to the provisions of the telecommunications interception test—that is, there is reasonable suspicion that that crime has been or is likely to be committed. So the power to seek warrants for surveillance devices—principally listening devices—has been with us since 1979, which is the same as for the telephone interception powers.

Senator LUDWIG—And that is without a warrant?

Mr Tinker—That is with a warrant.

Senator LUDWIG—I mean without a warrant?

Mr Tinker—Without a warrant?

Senator LUDWIG—This bill contemplates the use, in emergency circumstances—

Mr Tinker—You are talking about the emergency circumstances?

Senator LUDWIG—Yes.

Mr Tinker—I am sorry. No, that power has never been here, but this bill does introduce those powers.

Senator LUDWIG—I am trying to ascertain a justification for the use of that power. Where will the ACC utilise it, or doesn't it envisage that it would utilise the emergency power?

Mr Tinker—It would not utilise it regularly at all.

Mr Tebbet—The types of investigations that we are doing are proactive investigations; they are not reactive. For example, we may have physical surveillance on a particular subject or target. That subject or target goes to somewhere where we have a listening device installed under a warrant and some sort of a conspiracy then takes place. Evidence of that conspiracy is caught on a listening device that we have a warrant for and from that we understand that some other criminal activity is about to happen. That is the kind of reaction we need to be able to make. We need to be able to get around those particular conspirators with listening devices straightaway, otherwise we lose the acumen of the investigation, we lose that impetus and we also lose the evidence. It can be critical that we get around these people as a matter of urgency, and this bill provides for that.

Senator LUDWIG—In the circumstances that you have just outlined by way of example how long would it usually take you to get a telecommunications interception warrant in emerging circumstances, from your experience?

Mr Tinker—Those warrants are available to be sought Monday through Friday between the hours of, say, 8 a.m. and 7 p.m. whenever the AAT member is available and, prior to that, whenever the eligible Federal Court judge is available. The registries of both of those organisations also have after-hours contact points, and you can make contact after hours for that particular application. In extreme circumstances under the Telecommunications Interception Act, an application can be made and a warrant granted over the telephone.

Senator LUDWIG—How long does that take in emergency circumstances?

Mr Tinker—As long as it takes his honour to make up his mind at the end of the telephone call.

Senator LUDWIG—What is your usual experience of that? Have you sought those yourself?

Mr Tinker—Yes, I have sought those.

Senator LUDWIG—How long has that taken?

Mr Tinker—The administrative procedure after his honour makes up his mind takes longer than the telephone conversation.

Senator LUDWIG—So five minutes or 10 minutes at a maximum?

Mr Tinker—Yes. But they are very rare: they are usually in the middle of the night or in the early hours of the morning and they are usually only when circumstances are acute in terms of an operation that is being run on the ground at the time.

Senator LUDWIG—Has any ever been denied in your experience?

Mr Tinker—In my experience none have been denied in emergency applications.

Senator LUDWIG—You can appreciate that this bill introduces a slightly different regime to that of the Telecommunications Interception Act. Why wouldn't you choose to have the same regime? One of the issues in the back of my mind is that we will be back here with applications to vary the Telecommunications Interception Act to bring it into line with the SD Act, should it pass. I am trying to reason why, to avoid perhaps a tennis match between the act and the bill.

Mr Tinker—What specific issues do you have in mind?

Senator LUDWIG—The emergency procedure is different under the SD, some of the record keeping is different and some of the monitoring is different. There is no requirement for a civil offence if you use the powers under the SD inappropriately, whereas under the TI you can seek civil redress. There is a range of those sorts of minor issues, but they are relevant.

Mr Tebbet—This is much more a tactical issue and it is something that has to be done in the field, on the ground, whereas the telephone intercept is not—it is remote, it is removed, and it can be effected at any time. With this type of activity you are in the hands of the target as to whether you can put it into effect. You need to take the opportunity when it is presented, otherwise you may miss out and you may not be able to make that installation that could be crucial.

Senator LUDWIG—That is assuming that you are carrying the particular technology or the device?

Mr Tebbet—Exactly. And these operations need to be very carefully planned.

Mr Tinker—Another thing, Senator, is that the T(I) Act was written in 1979 and law enforcement has gone through substantial changes in the last 25 years, particularly with regard to privacy issues and the like. Also, this bill has perhaps been thought out on an extension basis, rather than the way the T(I) Act was written.

Mr Dargan—Perhaps some of the differences result from the different origins. For example, the Surveillance Devices Act was not really written from the ground up by the Commonwealth; it was partly adopted from a model developed by a joint working group and then, in a sense, modified to fit in with the Commonwealth legislative scheme. It reflects some of the provisions of the T(I) Act. So there would be those minor differences.

Senator LUDWIG—Then why would you want anyone in the ACC to seek a warrant for the implementation of a surveillance device? The way the bill is written—unless I am wrong—seems to indicate that any employee of the ACC can access a warrant.

Mr Tinker—Any member of staff of the ACC can apply for such a warrant.

Senator LUDWIG—Yes, that means any employee. So from the office staff to—

Mr Tinker—No, that in fact does not take place.

Senator LUDWIG—It may not take place but that is what the bill seems to suggest. I was trying to understand why you would require that.

Mr Tinker—I think it is in line with other law enforcement agencies where the power to apply for a particular warrant is given to a member—in other words, a constable or an

ordinary member. I think to further define a member of staff of the ACC may drill down a little bit too much in that it would be difficult to define a member of staff because the section would have to read 'other than a clerical officer'—or an attorney or somebody who might be employed in the registry—or something like that. All of the definitive powers of the ACC are given in all of the other acts to people who are defined as members of staff.

Senator LUDWIG—Who, from the ACC, would apply for warrants to utilise this power?

Mr Tinker—They would be police officers seconded from jurisdictions like the AFP, New South Wales Police, Victoria Police, WAPOL, SAPOL and QPOL. It is a practice within the ACC for no other person to apply for a warrant.

Senator LUDWIG—I see. Are there operational orders that require only those persons to exercise that power or seek a warrant?

Mr Tinker—Yes, there are, and there are also internal policies in the ACC that direct that.

Senator SCULLION—I am interested in the process for the Commonwealth Ombudsman. We are given assurances in the bill about information that has been collected after a certain period of time. There seem to be substantive auditing processes in place. There is always a culture within security and police forces: you guys are basically here to gather information. Intelligence is your game; that is the currency of most of your operations. It is very important. Intelligence and information: you put the blocks together and that is how you do your job.

Effectively, that particular provision of the bill is assuming that any information that is taken from a surveillance device will somehow be expunged from your minds. This is not going to happen—I accept that. But can you clarify the extent to which the auditing arrangements go? For example, if you gather some information through a surveillance device, subject to that information you then bring someone in for questioning, when it becomes overt, subject to that questioning, and there are notes taken by the police officers present in a record of interview. Clearly those questions relate to information that was gathered on the surveillance device. Are those notes audited? I have read the material and it just says there will be some auditing. For example, if it is a listening device, is it just the recording of that conversation? I have no understanding from the material I have about how far that will go and what the extent of the audit is.

Mr Tinker—In terms of the current provisions, any use of lawfully obtained information, particularly with regard to telephone intercept and listening device material, is treated—for example, with questioning and interviewing of suspects—as lawfully obtained information, and a specific record is made of that particular use of that material and that is included in the checking process by the Commonwealth Ombudsman whenever that material is utilised. It becomes what we call an LOI—lawfully obtained information—and a record is made every time, other than court proceedings, because it then becomes an issue in the court and the Ombudsman's reach does not go that far, other than to check every time the use of that lawfully obtained information is used. So, yes, there are safeguards and there are records kept of the use of that material.

Senator SCULLION—If, for example, you hear in a conversation, through a listening device, that Joe Bloggs in fact owned a giraffe, you say that as that is from a listening device that information is protected under the law, and we know that after a certain period of time

that will be audited and embargoed for certain things. But if in a record of interview you say to him, 'Listen, we understand that Joe Bloggs owned a giraffe,' and he knows that you have got that information and says, 'That's absolutely correct,' then that suddenly becomes lawful information that is not subject to the Commonwealth Ombudsman. Is that what you are telling me?

Mr Tinker—Yes, because it becomes part of a brief of evidence at that stage and becomes examinable by the court.

Senator SCULLION—That is if it proceeds to that point. At that stage it is only a record of interview. You may not seek to move to prosecute, particularly if this person is not necessarily involved directly in the crime.

Mr Tinker—That is true. Although, under those circumstances, if they are not necessarily involved in the crime but are a witness then that information in a witness statement is lawfully obtained information as well, and a record of that information that goes into the witness statement is made for the Ombudsman's certification.

Senator SCULLION—There is provision specifically for offences against the Fisheries Management Act. In both the explanatory memorandum and in the second reading speech for the bill it is mentioned that this specifically is intended to target the patagonian toothfish fisheries. I can only imagine surveillance devices would be things that would tell you where the vessel is. In my experience there has not been any allegation, rumour or suggestion that an Australian vessel has been involved in illegal taking of patagonian toothfish. How does this legislation enable us to place surveillance devices on people who are foreigners? They are not Australians, and the ships are not Australian. They are not operating out of Australia. Do you have any information on how a surveillance or listening device would be perceived in view of the fact that these are not Australian nationals?

Mr Dargan—The act provides in part 5 for the extraterritorial operation of warrants. That has some detailed provisions for when a warrant or a listening device or a surveillance device could be used in an extraterritorial situation like on a vessel. There are various requirements there.

Mr Tinker—The Customs Act does not hold extraterritorial powers and, as for the use of listening devices under the Customs Act for extraterritorial operations since 1979, it has been very difficult to lead that evidence in a trial here in Australia. In fact, it has not been done. This bill provides some assistance to the court in a future trial as to conversations that may take place on a vessel that might be 300 or 400 miles away from Australia on a mission to commit a crime within the Australian jurisdiction, so it is very helpful with regard to that. It really does not matter from where the vessel commenced its journey: in the case of Asian drugs, South-East Asia, or in the case of European drugs, Rotterdam, or in the case of cocaine, South America.

Senator SCULLION—So whilst this provision talks generally about an example such as the Fisheries Management Act, it could actually be extended to other areas where there was a need for a radio/satphone/seaphone interception?

Mr Tinker—Yes, absolutely.

Senator SCULLION—Okay, that was just not indicated in my material.

Senator MASON—Mr Tinker, I have a couple of questions following up those penetrating questions by Senator Ludwig about emergency authorisations. I can see this being an issue of concern to civil liberties groups. You mentioned that under current legislation you can already apply for a warrant by telephone. I think that, in response to Senator Ludwig's questions, you mentioned that process is very rare and that also no warrant has been denied—certainly to you. If that is right, why do you need this new power whereby you do not need to apply for a warrant at all except to seek the approval of an appropriate authorising officer? Why the need for the new process?

Mr Tinker—I spoke about applying for a warrant over the telephone to a judge or AAT member. That only relates to a telephone intercept warrant, not a surveillance device or listening device warrant. That power is not there at present under the Customs Act. I think this bill seeks to bring that type of power into line with the provisions in the Telecommunications (Interception) Act.

Senator MASON—So that is in line with standardising and regulating all the surveillance.

Mr Tinker—It is the foundation of applications.

CHAIR—Has not having the power caused you significant operational difficulty?

Mr Tinker—In terms of obtaining listening device warrants?

CHAIR—Yes, surveillance devices.

Mr Tinker—In terms of not having the power to get one over the telephone?

CHAIR—Yes.

Mr Tinker—Yes.

Senator MASON—How often?

Mr Tebbet—Loss of evidence and loss of intelligence. For example, if there is an opportunity to introduce an undercover operative into a meeting, that opportunity may come at any time and we would not be aware of that. We need to go to that meeting. We might need to record its audio and we might need to video it, to obtain images from that meeting. We need to be able to do that straightaway. We have not got time to really think about it, otherwise the opportunity is lost.

Senator MASON—So your evidence is that has affected your operational capacity?

Mr Tebbet—At times, yes. We have missed the window of opportunity at times, which can put the investigation back further. Rather than being able to clear the investigation up in a short period of time by being able to introduce some sort of technology, we have not been able to do that. We have had to wait until we get a warrant and then we have had to again wait for that opportunity to install, so we are missing the window of opportunity.

Mr Tinker—We tried to compensate for that loss, probably about seven or eight years ago when amendments were made to the Customs Act, for what we termed a 'person's warrant', rather than a named warrant. Those amendments allowed the use of listening devices on a particular person wherever that person moved to. That compensated quite well, but it still

didn't go to the lengths that this bill describes in an application for a warrant or seeking a warrant over the telephone, which this bill describes.

Senator MASON—Why are you applying for these new powers now? What is the rationale for making the application to the parliament for increased powers now? Any particular instance? Has any particular event caused you to seek these powers, or is it just a general evolution of increasing police powers?

Mr Tebbet—I think it is an evolution of technology, and being able to apply this new and emerging technology to improve the investigation capabilities. That is what it is about. I think what this legislation does is catch up with technology and methodology that we can apply to the investigations.

Mr Dargan—In a way it has been a long time coming. Under the Commonwealth legislation, like the existing Customs Act and AFP, they just have the ability to use a listening device only. Of course, these new technologies have been around for a long time now—10 or 15 years. So in a sense it is the Commonwealth legislation catching up with new technologies. Some of the states have already got comprehensive legislation where you can use a wide range of devices.

Mr Tinker—For some time you could apply for them. You can apply for them within the states over the telephone.

Senator MASON—Over the last 18 months this committee has looked at so much legislation giving increased powers to investigative agencies. I can see some witnesses here whom we have spoken to before. This committee has increasingly been asked to recommend to the Senate increased police or investigative powers. I cannot speak for the committee, but I am wondering if it will ever stop. Perhaps it will not. You are not using terrorism or the threat of terrorism as a window. What you are saying is that is nothing to do with that. This is simply a time when technology has to be captured by the legislation.

Mr Dargan—I think so. It has developed, as has been mentioned, from the joint working group model bill. That was finalised last year, and I understand some of the other jurisdictions are going through their own drafting and parliamentary process. So I think it is just more or less an historical accident, in the sense that it is happening now when there are other things. From our point of view there has been no particular operational incident that has caused us to ask for it now. We have been, in a sense, asking for these sorts of things for quite a while.

Mr Tinker—I do not think it is a unique application of power because there are other provisions of the Commonwealth law that grant emergency powers to police officers and members of the staff of the ACC. Nothing can be more sacred than a person's home, yet there are emergency search powers of that place, without a piece of paper, both in the state and in the Commonwealth arenas. And whilst they only get used very rarely, the powers are still there. I think this bill seeks to lift what was a lower bar to what law enforcement has available to it presently.

Senator MASON—The last couple of questions relate to what happens if you make a mistake. These marvellous notes prepared by the secretariat raise a very important issue. There is no civil remedy regime for aggrieved persons in this legislation as there is for unlawful deception or communication under the TI Act. What would be the grievance or

remedy procedure for people aggrieved by the use of this legislation? What remedy would they have?

Mr Tebbet—It would be much the same as if a police officer executes a search warrant on the wrong house and smashes the door in—'Sorry; we've made a mistake here. Wrong house.' That has occurred. It does occur. People are compensated for that.

Senator MASON—Remedies have not been taken away from people in terms of their capacity to sue civilly?

Mr Tinker—No.

Mr Dargan—I think it would be read in the context of the other, ordinary things that Bob has mentioned and the other complaints regime for the ACC. It is under the jurisdiction of the Ombudsman and the Ombudsman can come in and investigate complaints and investigate matters of his own initiative. I do not think this bill takes away any of that. All those existing checks and balances would still apply.

CHAIR—In relation to telecommunications interception there are specific remedies for unlawful surveillance and they are quite clearly set out in the T(I) Act. Why wouldn't they be replicated in this act, in relation to unlawful surveillance?

Mr Tinker—Civil remedies under the T(I) Act?

CHAIR—Yes.

Senator MASON—There is a regime in place. Why is that not being replicated here?

Mr Tinker—It has been some considerable time since I read the T(I) Act.

CHAIR—We get to look at it all the time, Mr Tinker.

Mr Tinker—I cannot put my mind to the particular provision.

Mr Tebbet—I also think that we have internal policies and procedures for the use of listening devices, physical surveillance and management of technical surveillance, and there are national operating guidelines that cover these things. Also, one just cannot go around the place putting these things in. It takes a lot of effort. It is usually a team effort of at least in the vicinity of seven to eight people to do a covert installation on somebody's dwelling house.

Senator LUDWIG—They did it in New South Wales in the 1980s.

Mr Tebbet—They did all sorts of things in the 1980s.

CHAIR—I am sure I can find a Queensland example, Senator Ludwig.

Mr Tebbet—I think that was before they had the New South Wales Listening Devices Act, wasn't it? There are certainly plenty of policies and procedures in place.

Senator LUDWIG—Yes, but who checks on that?

Mr Tinker—Certainly the Commonwealth Ombudsman.

Senator LUDWIG—Not on a warrantless surveillance.

Mr Tebbet—Under this legislation he will.

Senator LUDWIG—How will he check on that?

Mr Tinker—He will physically check the document trail.

CHAIR—What about where there is no warrant issued? There is no oversight of a process where there is no warrant issued.

Mr Tinker—That is a dilemma because the person—

Senator LUDWIG—It is, isn't it?

Mr Tebbet—It still has to be reported.

Mr Tinker—It has to be confirmed by affidavit within 48 hours, I think, before the AAT member that authorised the application over the telephone.

CHAIR—That is an emergency authorisation.

Mr Tinker—It follows on from the emergency authorisation.

CHAIR—Warrantless surveillance in and of itself does not require an application.

Mr Tebbet—What sort of surveillance?

CHAIR—Physical surveillance. There is no monitoring and no oversight of the extent of physical surveillance.

Mr Tinker—No. There are proximity issues. I can sit here and keep you under surveillance across the table and you can do likewise to me. Should we ask a court to be able to do that?

CHAIR—It is not a question of whether you might ask a court but to what extent records are kept—

Mr Tinker—Records are kept.

CHAIR—and what reports are made of activities in that sort of surveillance.

Mr Tebbet—The physical surveillance team's task is recorded on an official tasking form and that is tasked by the head of the investigation, so the physical surveillance cannot just run off at a whim and just decide to follow somebody or carry out surveillance. So they are tasked by the head of the investigation. During the course of surveillance they prepare running sheets which are contemporaneous notes which are treated as highly protected documents and those sorts of notes can become documents of the court and admitted into evidence.

CHAIR—Are they subject to any oversight? They are not reviewed by the Ombudsman or anything like that, are they?

Mr Tinker—No.

CHAIR—As I understand from my most recent reading of the T(I) Act, all applications for a telecommunications interception have to be supported by an affidavit.

Mr Tinker—Yes.

CHAIR—Is there any reason why you would not replicate that requirement even in relation to emergency authorisations? Why shouldn't you need an affidavit for an emergency authorisation under this act?

Mr Tinker—The emergency authorisation may take place in the middle of the evening or in the early hours of the morning.

CHAIR—Do TI applications take place in the middle of the evening or in the early hours of the morning?

Mr Tinker—Emergency ones do, yes, over the telephone.

CHAIR—But they still need an affidavit?

Mr Tinker—I think the T(I) Act says within 24 hours. I think this act says 48 hours. So they are followed up with affidavit evidence to the same issuing officer.

CHAIR—From your perspective, do you think it will matter if the two pieces of legislation are identical in the requirements for time frame, issuing officer and so on?

Mr Tinker—Having had to prepare applications within 24 hours for emergency telephone intercepts it is not a long time in which to prepare that information to give to the issuing officer, who may have been spoken to at 5 a.m. You have until 5 a.m. in the next 24-hour period to give it to him. If the T(I) Act were to amend to the same time limit as this act it would be easier.

CHAIR—Mr Tinker, I suspect the committee is not going to go in that direction. We are unlikely to put in new ideas for you.

Mr Tebbet—It is a different thing altogether. We might need to cover one meeting once and we will get only one opportunity to do it, and that meeting may be on in 10 minutes. Whereas with a telephone intercept—

CHAIR—I see. That is the sort of operational information that we need you to tell us.

Mr Tebbet—That is how it works. For example, we might have a target who gets on a plane in Perth to fly to Sydney. The physical surveillance will put the target to the plane and the physical surveillance in Sydney will pick up that target. They will do the surveillance on them, and they might go to a place and meet. We might get off a telephone intercept the fact that they are going to meet and discuss certain criminal activity. We need to be able to respond to that straightaway. If we can we need to get that device into that centre of conversation. We might not know where that is until 10 minutes before the meeting takes place. So it is about being proactive and reactive. That is where we fall down at the moment, because we just cannot do that.

CHAIR—They are useful points for us. Following on from what Senator Mason was saying, we have spent literally the last 18 months to two years considering bill after bill after bill seeking further powers and extensions of powers for law enforcement agencies in this country. That is what they do and that is what we do. What we now have in front of us is a whole new grab bag of powers, devices, new methods of authorisation and permission being sought to do things. So we have TI warrants, surveillance device warrants and even search warrants lined up operationally. What is to stop a law enforcement agency from just making a whole range of applications across the board to see which one comes home a winner?

Senator SCULLION—Warrant shopping.

CHAIR—Yes, that is a good turn of phrase, Senator Scullion.

Mr Tebbet—There is nothing to stop an agency from going warrant shopping except that you need to be able to resource these things. The installation of a listening device is a very

lengthy process. For example, to install a listening device in your house we need to control you and all the other occupants of the house so that we can do it. If the place has an alarm or has high-security locks we need to address those issues. People need to be trained to be able to do that. People need to be able to do it covertly, without being detected. We need to be able to service that device if something happens to it. It is a very lengthy process for which you need people who are highly skilled, and you need to be able to manage it. It is risky. One slip-up and our operation, which may have taken six months to get to that point, is gone. So we cannot do these things lightly, because they need to be very carefully and tactically planned. There are not a lot of people around with the skills and expertise in this business. It regulates itself and the ACC, like everybody else, does not have the resources to put about the place, so we must be very strategic in how we deploy this kind of methodology in our investigation.

Mr Tinker—Things that are not normally seen are the affidavits applying for these warrants. They are subject to PII claims within the court, if they are requested, and they are very hardly defended in terms of the information that is in those affidavits. The test before an eligible judge of the Federal Court or a member of the AAT is very high on reading that affidavit. I have had affidavits rejected on the basis that his honour did not feel that there was sufficient reasonable suspicion. So you take your affidavit away, do a bit more work and find a little bit more that you can put in the affidavit. They are not easy applications. None of these issues is easy in terms of law enforcement activity. If you look at the Hollywood scene in terms of law enforcement, what they try to squeeze into one hour may be nine months work. I suppose what Mr Tebbet is saying is that we do not do these things lightly and, when we do do them, in our opinion we do them very properly. They are transparent, they are examinable by the ombudsman, either state or Commonwealth—whichever jurisdiction the warrant is taken out in—and the big test at the end of the day is what his honour is going to say at a trial.

Senator SCULLION—I think the issue here is really that I may have complete confidence in myself and in all the enforcement agencies—and they are doing the right thing; there is no doubt about that—but there are organisations that take it upon themselves to ensure that that is the case. Civil Liberties Victoria and a whole bunch of people make sure that that is the case. I want to talk about forum shopping. If we had consistency, whether it was for a search warrant, a surveillance device warrant or a telecommunications intercept warrant, I think they would be a lot happier because, whatever the provisions, they would be transparent and they would be the same. So, if I got a search warrant, it would only be because that was the specific area in an operational sense that I wanted to take care of, surveillance devices would only be for specific areas where those devices needed to be used appropriately, and the same would be the case for telecommunications devices. I think that would be preferable to the perception that there was the possibility of saying: 'Do I get a surveillance device or a telecommunications device? A telecommunications device involves a 24-hour affidavit, this one involves a 48-hour affidavit, so let's go for the 48-hour warrant because I am absolutely flat out.' In an operational sense, I understand about the resourcing—and I think you made some very appropriate remarks—but my question is: would you have any problem with consistency across all operations?

Mr Tinker—None. It would make an investigator's life easier if it were consistent across the board.

Senator LUDWIG—Which way, though?

CHAIR—There may be one other issue that we will follow up on notice, if that is okay, and if anything comes out of the rest of our examination this morning we may pursue that with you by way of questions on notice. The reporting date is later in the month so we will come back to you as soon as we possibly can if we need to. If there are no further questions, I thank Mr Dargan, Mr Tebbet and Mr Tinker very much for assisting the committee. It is a pleasure to hear from the ACC. I am not sure that the committee has had the ACC before it in recent times in a hearing such as this, so thank you very much for your assistance.

[10.20 a.m.]

BERNIE, Mr David Michael, Vice President, New South Wales Council for Civil Liberties

CHAIR—I welcome by teleconference Mr David Bernie. We have received a submission from the council which we have numbered 3. Do you wish to make any amendments or alterations to that submission?

Mr Bernie—No, thanks.

CHAIR—I invite you to make some opening remarks and at the conclusion of those we will go to questions.

Mr Bernie—Our concerns are general concerns. We would like more time, obviously, to go over the details and if there is something that you would particularly like us to go to we could go to that in more detail but we would need some more time to do it. Going through our general concerns, we are concerned obviously about further increasing surveillance over Australian citizens but recognise, of course, that with the technology that is becoming available law enforcement authorities are going to want to use such technology and so it is best that it be regulated by some sort of legislation like this. In approaching that, we think it is important that there be as much control over that outside the executive as is practically possible.

I notice that the bill provides for the warrants to respectively be issued by a judge or members of the AAT. We are a little bit concerned about the members of the AAT being able to authorise warrants. We have found with regard to listening devices and telephone interception matters that since members of the AAT have been authorised to issue such warrants there has been quite a blow-out in the number of warrants that have been issued. It is hard to make some sort of qualitative research about all of that—and I am not being disrespectful to members of the AAT who do quite a good job as far as the tribunal is concerned, but they are a little bit closer to the executive government than, say, a judge. So in our submission, as far as the issues of warrants go, we say that it should be judges and not members of the AAT.

Another thing that we are concerned about here, and I think we have referred to it in our submission, is that although various offences are put up for the misuse of information there is not actually an offence that I can see in there—and you might be able to point me to one—about breaches of conditions of the code that is effectively set up here by the authorities, if they breach those conditions themselves in terms of doing unauthorised tapping. So there is section 45 dealing with unauthorised release of information once it has been obtained but there seems to be nothing actually dealing with penalties for authorities in going and doing tapping or surveillance which is in breach of the code overall—not that I could see anyway. Also, we must be careful, of course, that there is some sort of statutory protection for whistleblowers. We would like to see that so that they do not get caught up, for instance, in the offence provisions in section 45 of the proposed act.

Another area of concern is about passing on information to foreign governments. I know that this is determined there; it is referred to in section 45(5)(f). Obviously this has to be read jointly with the Mutual Assistance in Criminal Matters Act as well, and I have not been able to go to all of that. But one of our concerns would be that you could have surveillance of Australian citizens being passed to foreign governments, and it does not really qualify which foreign governments they are. We may not be concerned about surveillance being passed on to the US government or the British government or the French government but we might have concerns about surveillance information being passed on to, say, the Pakistani government or the Saudi government in respect of activities of Australian citizens in Australia and how that information might be used by those governments which do not have the same sorts of democratic systems that we are used to. In particular, the way that it is dealt with there is by reference to an offence punishable by three years imprisonment or more. In some of these countries some very minor offences are punishable by three years imprisonment or more. Indeed, it even refers to punishment by death. Given the Australian government's stand in relation to the death penalty, we would want to be very careful that we are not handing over information which could be about surveillance of Australian citizens which may even be leaving them liable to the death penalty in a foreign jurisdiction. So that is another area of concern. They are the main areas of concern that I wanted to point to at this stage.

CHAIR—I will start by asking you the question we have just asked the Australian Crime Commission. In comparison with the Telecommunications (Interception) Act, which contains a civil remedy regime for persons who are aggrieved under the legislation, this legislation does not have a similar set of provisions. Does the CCL have a view on that?

Mr Bernie—We think that people should be able to launch such action and, indeed, going through the legislation I could not see that there was any provision for that. I would have thought that if it were not addressed it would not take away a person's right to sue civilly but, as you will know, under Australian law there is no definite right to privacy. There have been some statutory extensions of that—for instance, with the Privacy Act. But I think it would be better if it were made clear in the bill that in the case of abuse there is a civil right for people who have been damaged by breach of these conditions.

CHAIR—Thank you for clarifying that.

Senator LUDWIG—Following up on that question from Senator Payne, if a person, for argument's sake, executed a warrant and knocked down the wrong door to a house then there is a civil remedy available because of the tort of damage and—

Mr Bernie—Yes, trespass.

Senator LUDWIG—But if a surveillance device was used at the wrong address and information was obtained, would there be a civil right to—

Mr Bernie—It would be very questionable. As I said, there is no common law right to privacy per se. We seem to be seeing here in Australia, even as we speak, incremental increases by the courts in respect of that, but it is still the situation that there is no tort of invasion of privacy as such. I think it should be given some consideration. Obviously, in terms of general law it is a state government matter as to whether that should be done. But, until that

is done, to make it clear that people do have a civil remedy it would be better if that were actually inscribed in the act.

I do see a problem here. If you go to the wrong address it is quite clear to the person when you have gone to the wrong address that you have been there. It is not immediately clear to people, though, that they are being wrongfully surveilled or have been subjected to surveillance in the same way unless it somehow becomes obvious to them in the future. Nevertheless, I think it is important that such a remedy is put into the legislation. I was talking about enforcement, and putting in such a remedy highlights to agencies that they could be liable if they do not abide by the conditions set out in the code.

Senator LUDWIG—Additionally, the legislation provides now for a new power which is an application for surveillance to be authorised in emergency situations. I know that you have not had a lot of time to look at this, but I was interested in your comments about whether this provision is structured in such a way to ensure that it has relevant accountability mechanisms attached to it and that, in addition, it provides for the minister to be advised about the use of this power and whether it is appropriate in all the circumstances.

Mr Bernie—This is the worry. As I say, our general approach here is that, rather than the minister being advised—indeed, it could be prejudicial, as we say, to the minister being involved—judicial surveillance would be better than ministerial surveillance.

Senator LUDWIG—Why do you say that?

Mr Bernie—My view is to move the supervision of the surveillance procedures into something away from the political structure and the executive government.

Senator LUDWIG—When you say supervision by the judiciary, do you mean in the sense that the warrant is then justified later?

Mr Bernie—Yes. I understand that in these emergency situations they must apply for an authorisation within two business days. I think that is best done through a judicial process rather than a ministerial process. Our other concern was about what happens to the material that has been collected in those circumstances if the approval is turned down.

Senator LUDWIG—I notice the Ombudsman has some power of external oversight. Do you think that is sufficient in terms of the broad reach of this bill?

Mr Bernie—I think so—together with parliamentary oversight. I think it should be, and I would have thought that would have been provided for. There should be parliamentary oversight as well. I think it would be useful to have public reports going to the number of warrants that have been issued with as much detail as can made public without prejudicing ongoing investigations. These new bits of technology mean this is an area of incredible power and incredible surveillance. They are quite impressive but they also give incredible powers of surveillance, and I think it is important that in addition to the Ombudsman's scrutiny there be parliamentary scrutiny on an ongoing basis and an annual report, for instance, as to the number of these warrants that are being issued. There should be more detail when possible when it does not prejudice ongoing investigations.

Senator LUDWIG—Is the provision of a parliamentary report in the order of what is provided under the Telecommunications (Interception) Act?

Mr Bernie—Yes. At least it gives some quantitative analysis. As I said before, it is hard to do a qualitative analysis without knowing what it is all about. I realise that government departments and authorities and law enforcement agencies are always loath to give any more information and will always say that they are prejudicial to ongoing investigations. I would have thought that after a certain period of time more information might be given out about the details of the warrants without actually issuing names and specific addresses. There could be more details about what sorts of warrants are being issued and in what sorts of circumstances they are being issued. That would be useful for us to make some sort of qualitative analysis of where we are going with all these warrants.

Senator LUDWIG—You would also like to see, as I understand it, how they deal with the information once obtained.

Mr Bernie—Yes. That is a big privacy concern not just in this area but in gaining information in general. Also of concern are how that information is dealt with and how it is secured. Yes, that is also an area of concern.

Senator LUDWIG—Thank you.

Senator SCULLION—The previous group that gave evidence were from the Australian Crime Commission. It was interesting to talk to them about their views on the consistency of legislation. In your submission I think you touched on the difference between the process of the telecommunications (interception) bill and that of the bill before us now. Could you expand on some of the areas of consistency of the legislation and say how you think that may be important?

Mr Bernie—I can understand that they would like to see a more consistent approach, but we should not in the name of consistency have a lax approach—let's put it that way. The area where it appears to be consistent, as I have indicated before, is that in the proposed bill members of the AAT will be able to grant warrants as is the case under the Telecommunications (Interception) Act regime. That is an area of concern. We would like to see it limited to judges in both cases. I have to admit that I would need to take some time to go to the other areas because I am not aware of all the details in relation to the other areas where there would be inconsistencies. But I can certainly see that there is something to be said about having a consistent approach to both telephone interception and surveillance.

Senator SCULLION—You also submit that section 46 should be amended to require independent oversight—by the Ombudsman, for example—of any decision by police to destroy surveillance records prior to their destruction. In view of the auditing requirement by the Ombudsman with regard to records and evidence that has just been given about the way in which information from surveillance operations can be changed into lawfully gained information, in the sense that parts of the records of interviews that happened prior to that and may have involved information gained from the surveillance device are outside the purview of the Ombudsman, how useful do you think that is going to be?

Mr Bernie—That could be an area of concern. If that is the case you would want those records destroyed as well. I realise there would be a real reluctance to do so. From my dealings with the police authorities I think they have a real reluctance to destroy anything they get. They always feel something is going to be useful somewhere down the track. But I think

it would be useful if that were expanded to make sure that that other material was destroyed as well.

Senator SCULLION—I wonder about the capacity to do so, given the nature of those investigations. I imagine that there would be some material that was associated with a surveillance device or a telecommunications intercept but there would also be much information that was not necessarily associated with, or gleaned from, those things. With the difficulty in asking the enforcement agencies or intelligence gathering agencies to somehow differentiate whether information that has been gained from questioning someone was gained as a direct consequence of a surveillance device, I see such a grey area that I do not know if it would ever be possible.

Mr Bernie—Yes, it is difficult. If they have obtained information and it has gone into the police officer's head, for instance, they obviously cannot erase it. That is always a problem in drawing lines about this sort of area but I suppose we have to draw a line somewhere. It is very difficult to say for certain but it shows you the overall need in terms of concern in this area. Once information is gained it is gained and possibly, even though that information might have been destroyed, the basic parts of that information are still known to the authorities, particularly investigating officers. It is quite human that they would then use what they know as part of other investigation techniques, as you say. If they are conducting an interview and they say, 'Isn't it true that you went down such and such a street on such and such a day,' suddenly, as a result of that, the person being interviewed will think that they have been under surveillance and it may affect the whole way the interview goes. In a perfect world you could somehow bring all of that under control, but we have got to draw the line somewhere.

Senator SCULLION—As I understand it, the Ombudsman now conducts an audit of the materials that have been specifically gained. I am not talking about physical observation; I am talking about material from surveillance devices, like a video recording or a sound recording of a conversation. The Ombudsman will, as you say, be taking an audit of how that is stored and the fact that it has been destroyed if it is no longer needed. In view of the issues of difficulty in other areas, why do you think that the Ombudsman's audit would not be sufficient in those cases?

Mr Bernie—I would prefer it if somebody from the Ombudsman's office did witness the destruction of that material. I acted on an audit committee in relation to CCTV cameras in the city of Sydney. When any of the tapes were to be destroyed, a member of the audit committee would attend upon it. It does not have to be the Ombudsman personally but, talking of outside supervision of what is going on, I think that somebody from outside the police or the Crime Commission—so somebody from the Ombudsman's office—should attend while that material is destroyed. That would be my preference.

Senator MASON—I have one question and I would perhaps make one observation. In response to some questions from Senator Ludwig, you mentioned the general proposition that there should be judicial rather than executive oversight of surveillance technologies.

Mr Bernie—Yes.

Senator MASON—I think that is fair enough. In your opening address I think you mentioned that you would prefer to have judicial officers rather than members of the AAT administering that process.

Mr Bernie—Yes.

Senator MASON—I understand why, but is that practical?

Mr Bernie—I think it is practical. I do not think there was too much difficulty in terms of getting warrants prior to the amendments to the telephone communications interception procedures. I am sure the police would probably tell you something else, but I think it is practical. There are enough federal judges around, and I would have thought that state judges could also be deputised with federal jurisdiction in relation to this. As I said, without meaning any disrespect to members of the AAT, they do rely on reappointment by the government and they are closer to the government. In the overall scheme of things, in terms of supervision of this process, I think it would be best that you have it somewhat removed from the executive branch, and that would be done by giving it to judges to do. As I say, with all respect to them, members of the AAT are a bit closer to the executive branch. I do not think it would be impractical. I think that there would be enough judges, both state and federal, who would be able to do it.

Senator MASON—I bet you they would love the task as well, wouldn't they?

Mr Bernie—I do not think they would. I notice the judge has to sign a consent to do so. But I think judges are fairly well remunerated, and it is part of their job. It has traditionally been part of the job. It has always been a funny thing, when you really think about the issue of warrants and judges, but that has been a traditional part of a judge's job in oversight of the warrant procedure, starting with search warrants. I think it should be the way we approach it with regard to this as well.

Senator MASON—As an observation, there has been a bit of discussion this morning about the tort of invasion of privacy, which the Americans have perfected, along with their constitutional right to privacy. Hasn't the House of Lords just knocked it on the head with Ms Naomi Campbell?

Mr Bernie—Yes, but even there it is somewhat restricted. I understand that the *Daily Mirror* publishers are going to take it to the European Court of Justice. I am not sure on what provision—probably the right of expression under the European human rights scheme. So that will be interesting to see. As I understand it, US Supreme Court decisions about right to privacy have certainly been used to strike down, for instance, criminal laws which were considered to infringe that area.

The Americans had this problem too with their first amendment right, being the right of free speech, conflicting with the concept of right to privacy. Even the United States has not really got to the stage where invasion of privacy is seen in all jurisdictions as being a right in itself. It is a much more litigation friendly society and, in a society where, in their judicial law making, they are more likely to be creative, it has certainly gone a lot further than we have.

As you know, we have a Privacy Act at a federal level and we have various pieces of state legislation, but none of them has gone so far as to actually give a civil right of privacy. I

would like to see something along those lines, but it does not exist at present. It certainly has not been the common law position, unless you could tie it in with something like 'nuisance' or 'trespass' or those other torts—and not all invasions of privacy involve those.

Senator MASON—It will be interesting if it is going to the European court. You are right that there is a right to freedom of expression under their covenant, but there is also a right to privacy. I do not know how they can resolve that.

Mr Bernie—Yes. Indeed, this is an area for the Council for Civil Liberties. This is a conceptual problem. We obviously support the right of freedom of expression—and, for the most part, the mass media take most of that up—but when does it go too far and get into a right to privacy? And we also support the right to privacy. Balancing those rights can be difficult in some areas. I think one reason that governments have not rushed to enact a tort of invasion of privacy is that they are unsure where it would end. I certainly would say that it should be made clear, at least as far as this legislation is concerned, that any breach of the legislation would give rise to a civil action by any aggrieved person.

Senator MASON—Okay. Thanks very much.

Mr Bernie—Thank you.

CHAIR—Thank you very much, Mr Bernie. That concludes the committee's questions. We appreciate both your submission and your assistance this morning.

[10.48 a.m.]

CHADWICK, Mr Paul, Privacy Commissioner, Office of the Victorian Privacy Commissioner

FISHER, Ms Michelle, Manager, Policy, Office of the Victorian Privacy Commissioner

CHAIR—I welcome by teleconference Mr Paul Chadwick and Ms Michelle Fisher. Privacy Victoria has lodged a submission with the committee which we have numbered four. Do you need to make any amendments or alterations to that submission?

Mr Chadwick—No, thank you.

CHAIR—I ask you to make a brief opening statement, and at the conclusion of that we will go to questions from the committee. Please go ahead.

Mr Chadwick—Good morning, senators. Thank you for the opportunity to address you. May I make it clear, first of all, that the Office of the Victorian Privacy Commissioner is an independent statutory office and I do not appear, in any representative sense, for the government of Victoria. The Victorian Information Privacy Act 2000 has various functions for the Privacy Commissioner, and one of them is to make submissions as appropriate to raise awareness and understanding of privacy issues. It was in that role that I acted in submitting to this committee; it is something that of course I do more regularly to the Victorian parliamentary committees. As a courtesy, I discussed the notion of making a submission with the Federal Privacy Commissioner, or the Acting Federal Privacy Commissioner, as it is at the moment.

On the bill that is before you I will make a couple of broad points. First, part of my submission intends to draw this committee's attention to the divergences that have already occurred between the model bill in this area—only very recently developed by a joint working party of Commonwealth, state and territory representatives—and, on the one hand, this bill and, on the other, the Victorian bill that went through the Victorian Legislative Assembly last week. Those divergences are disappointing in the sense that they are not very well understood or debated. They are also disappointing on another level, of course—something familiar to all of us—namely, the difficulty of achieving in the federation some kind of harmony in pieces of law that ought to work more smoothly across borders.

The second general point is that it is essential that the parliaments of Australia grapple with new and converging technologies in this area. It is essential because we need better law enforcement in these times and we need the capacity to exploit the technologies. We also need better accountability of law enforcement agencies as they exploit the capacity of these technologies. There are a couple of leading cases in other jurisdictions. One I have referred to: the US case of Kyllo. There is also the Canadian case of the Crown and Duarte. Cases such as those are fairly recent analyses of these issues. They stress the speed with which the technologies are developing. I do not think the current bill has addressed that adequately.

I think it is worth taking a historical look and seeing that Anglo-Australian law generally has tried to address the question of state surveillance of the citizen in stops and starts that tend to parallel developments in technology. So, for example, the ubiquity of the mail led to attention in English law to questions of opening of the mail and privacy. The next great

development was of course the technological development of the wiretap. With the development of listening devices and wiretaps we saw a flurry of activity in the courts in the early 20th century around privacy and the limitations on the state's surveillance of the citizen.

Next was a relatively recent flurry of activity, evidenced in Victoria in the Surveillance Devices Act 1999, where there was an attempt to move away from just thinking of surveillance in terms of listening devices, telephones et cetera and towards thinking about optical surveillance and trying for a technology neutral approach. I suggest that we need to now think fairly carefully about another burst of activity. That is an attempt to take into account not just technologies that listen but also technologies that look; technologies that locate an individual's car or other consumer item; technologies that track the location of a citizen; and technologies that exploit the fruits of many computer systems which, when the information is put together, can lead to fairly sophisticated surveillance of a person.

Another and distinct point, which we can return to at your pleasure, relates to some of the differences in the Commonwealth bill which seem to vary even from the model bill's recommendations. One important one is the possibility of not having police specify the object or system that is to be used to transmit information. That would appear to allow use of home entertainment systems—an individual's web cam, for example—which can be remotely activated. Those sorts of items could become surveillance devices for the purposes of law enforcement. There may be many proper reasons for that. I do not dispute that at all. But they should be contemplated by law-makers in setting up a balanced system in this area.

I urge on the committee that there be no warrantless use of surveillance devices under law. There is a value in the scrutiny that the judicial branch applies to the executive branch, especially in this area of surveillance. If we were to permit warrantless use by police of surveillance devices then at a minimum we need better oversight than the current bill provides. That would include, firstly, compulsory provision of information to the Ombudsman with much more fine-grained oversight provisions than the bill currently has; secondly, the compulsory provision of information about warrantless surveillance—at the moment the bill only requires provision of information about warranted surveillance; thirdly, clear power for the Ombudsman to scrutinise the information given—that is, a strong power for the Ombudsman to go in and check; and, fourthly, of course, published reports to the parliament, as long as that does not undercut the efficacy of the surveillance itself—a standard approach.

I also ask the committee to differentiate in its thinking between the acts of surveillance that the state may undertake and the state's use of the fruits of that surveillance. I think it is healthy in this area to hold those two categories in mind and to differentiate them. Firstly, I would like to acknowledge the clear public interest in appropriate authorities using surveillance devices and surveillance techniques under law. There is no doubt that it is in the public interest that that is required at times. Secondly, I would note that we have clear lessons from history that that kind of power can be abused, including by law enforcement authorities.

Thirdly, I think it is fair to say that there is a general understanding of the idea—and certainly there is literature that supports it—that surveillance can distort both the watcher and the watched. There are some fine analyses of the effects of insufficiently accountable surveillance activities, for example, in the former eastern Europe. Two very fine examples are Anna Funder's book *Stasiland: true stories from behind the Berlin Wall* and Timothy Garton

Ash's book *The file: a personal history*. These are serious analyses of the effects of state surveillance when it is not properly accountable under law. I do not suggest for a moment that what they lay out there is something that can be expected in Australia. I am suggesting that there are lessons to be learned from the experience in other jurisdictions about the importance of getting the balance right and the oversight right.

Fourthly, I think the legitimacy of the state's surveillance of the population, which always turns on trust to some extent, is supported not only where the surveillance is done under law but also where the law travels alongside the surveillance in a practical way. What I mean by that is we ensure that ombudsmen, other accountability bodies or the courts are travelling alongside the police and other agencies as they use the powers that the parliament confers to surveil the population.

Lastly, I think it would be consistent with the learning underneath these sorts of bills and with the law as it has developed through the courts over the decades that, if this bill were to include in its objects section an express reference to Australia's obligations under article 12 of the Universal Declaration of Human Rights and under article 17 of the ICCPR—to put it in short: to respect privacy—and an express acknowledgment that a balance must be struck, that may assist in the detailed administration of this law over time. Thanks for your attention.

CHAIR—Thank you very much, Mr Chadwick, for both your comprehensive submission and your remarks this morning. Ms Fisher, did you wish to add anything at this stage?

Ms Fisher—No, thank you.

CHAIR—We will go to questions.

Senator LUDWIG—I assume that the Victorian bill you mentioned is now an act?

Mr Chadwick—It has only gone through the lower house; it is not yet through the upper house.

Senator LUDWIG—To what extent does it—and perhaps you can be brief—diverge from the model bill?

Mr Chadwick—I will ask Michelle Fisher to take that issue on. She has followed the detail.

Ms Fisher—The Victorian bill departed from the model bill in at least a few respects. The first is the definition of tracking device. The Victorian Surveillance Devices Act currently has a different definition of tracking device than is proposed in the model bill and they have declined to alter that in accordance with the joint working group's recommendations. They accepted that 'tracking device' is limited to devices where the primary purpose is to track or locate an object or a person, which leaves open the surveillance of devices that have other purposes. Those are not regulated by the legislation at the moment, and that is not going to change under the current bill.

A couple of recent amendments have been introduced while the bill has travelled through the lower house, partly I suppose in response to the Commonwealth bill. One of those changes allows for remote surveillance where there is a concern about personal safety in relation to listening to words spoken and participant monitoring. Another takes up the same

amendment proposed in the Commonwealth bill in relation to the use of systems such as home entertainment systems—to activate or operate surveillance devices.

Senator LUDWIG—Are they the substantive changes?

Ms Fisher—Yes, those are the amendments that have been accepted in the lower house.

Senator LUDWIG—In respect of objects, does the Victorian bill include the privacy issue that you mentioned earlier?

Ms Fisher—No, it does not.

Senator LUDWIG—In respect of the adoption of warrantless surveillance, is that similar to that which was provided for in this bill?

Ms Fisher—It departed in some respects. I understand that further amendments were proposed as the bill travelled through the upper house, and they have not been made public as yet. But there certainly have been some references in the press to the amendments that have been put in the Commonwealth bill in relation to warrantless surveillance, where it does not involve trespass et cetera.

Senator LUDWIG—To encapsulate what you are saying, if this is right, the Victorian model bill is closer to the joint working group model bill than the current bill before us, but, whilst it is tracking its way through the Victorian parliamentary system, it is converging in some areas such as the use of warrantless surveillance and perhaps some other matters as well.

Ms Fisher—That seems to be correct.

Senator LUDWIG—But they are not uniform in that sense between the Victorian bill and the bill before us.

Ms Fisher—Not the currently accepted amendments, but I cannot comment on the proposed amendments.

Senator LUDWIG—Could you take it on notice to provide that information when the proposed amendments are available? I do not want to put you to too much trouble, but if you would not mind advising the secretariat we could follow up on that, just to see which way the Victorian legislation is heading.

Ms Fisher—I am happy to.

Senator LUDWIG—Thank you. In respect of the use of warrantless surveillance, as proposed under the Victorian bill, is any proposal included in that for monitoring or checking or even ensuring that it is accountable?

Ms Fisher—The Victorian legislation, as I recall—and I would have to go back to check on it to be sure—is similar to the Commonwealth legislation. The accountability measures are tied to warranted surveillance and do not apply to situations where the surveillance is without warrant. So the aspects of inspection and the reporting to ministers and parliaments do not encompass warrantless surveillance.

Senator LUDWIG—I know that you may not have all the information about the Victorian bill before you, so if you want to defer and take that on notice I am happy for that to occur.

The other area that I am interested is in relation to the keeping of records. I take it that you are in favour of the destruction of surveillance records and reports, as detailed in your submission. Was that originally part of the joint working group model?

Ms Fisher—I do not think they addressed that particular issue about having oversight prior to destruction of records.

Mr Chadwick—It is a very standard data protection type principle. The difficulty in commenting in this area is that one needs to know what public interest retention serves. As you would see from the submission, Victoria has had some experience of retention of personal information by police for a long period where the Ombudsman has expressed certain concerns about that. There have also been concerns about situations where destruction was said to have occurred but did not or where retention regimes, if one could put it broadly, might not have been as effective as they could have been.

This area is one that deserves attention because these sorts of records live on and because, as the senators would know, one of the stated reasons for this revisiting and reform of surveillance devices legislation around the country is the concern about dealing with terrorism. As senators would know, particularly those who served on the relevant committee, the definition of 'terrorism' is a contested issue in many jurisdictions and tends to require fine judgments at times. It is for those reasons that one turns one's mind to how long material might be kept and what kind of security or oversight regimes ought to be applied, because it can have very pejorative or harmful effects on a person in the long run as well.

Senator SCULLION—I want to get some clarification on one assertion in your submission. It says:

> While the Bill proposes to regulate the use of data, optical and listening surveillance devices and tracking devices in much the same way that telephone tapping is regulated by the Telecommunications (Interception) Act 1979. (TI Act). The issue of warrants by members of the AAT has seen a great increase in telephone warrants.

I wonder if you could clarify the point you are making there. I am assuming that the point is that the AAT is now associated with it and there has been an inappropriate increase in telephone warrants. I just want you to clarify that for me if you could.

Mr Chadwick—I do not think that is our submission. Michelle is indicating to me that you are quoting from something other than our submission. I would be happy to clarify if it was from us, but I do not think it is.

Senator SCULLION—You are quite correct. I apologise.

CHAIR—At the moment, in terms of the operations of law enforcement agencies in this area, there is not a comprehensive set of regulations and guidelines. Is it Privacy Victoria's view that the provisions of this bill go a distance towards improving the positions of citizens who might be affected by the use of surveillance devices?

Mr Chadwick—What I think improves matters is this kind of scrutiny that you are now engaging in. I think that goes to the legitimacy point. I do not think any of us dispute two key points: the powers are necessary, although we all feel uneasy about them; and the potential for abuse is real. Both of those things, I think, are accepted by all parties who come to this debate

in good faith. Firstly, concern can start to develop in discussions like this where the activity is seen to be hasty. There was not much time for consideration of and comment on the joint working party's discussion paper. That itself was of concern. Secondly, there seem to be divergences from a model that did have, to some extent, a preparation period. You are left with a fairly swift period of time in which to apply what one might call the parliamentary sieve to satisfy yourselves and report back to the Senate on matters raised by this bill. They are not simple matters. Also, as we have tried to point out, there is a large amount of literature on the possibility of different technologies being used for surveillance. I think the answer to your question is: yes, this kind of process does improve matters, but it could have been better.

CHAIR—Thank you very much for that observation.

Senator MASON—On that point, in your opening remarks you spoke about the developing ubiquity of the mail system and protections being garnered to protect the mail. In more recent times we have had wire tapping and bugging, and now we have infra-red technology. I suspect that you will be very busy in the years ahead as an advocate for privacy protection as the technology and the promiscuous exchange of information continue to get faster and faster.

Mr Chadwick—Like any statutory officer, I am limited by the act that creates the office. Part of the objective of the Victorian act is a recognition of balance. It is stated very plainly that the Information Privacy Act in Victoria does not see privacy as some kind of absolute or some kind of trump. I know these are truisms for you, but it is worth adding them to the record. The Privacy Commissioner has to strive for balance in these sorts of situations where, if you like, law is on the anvil and getting hammered out. I think it is important that the Privacy Commissioner animate the privacy considerations where, in the spectrum of views that the decision makers are receiving, there is a clear voice for what one might call 'other public interests'. You have heard clear voices for law enforcement and security interests; it is important for the Privacy Commissioner to animate these other options.

Senator MASON—So you see yourself not as an advocate for privacy but rather as giving perspective to the issue?

Mr Chadwick—We must, first of all, try to animate the privacy interest. It is a legitimate interest protected under law—and protected under international law and international instruments to which Australia subscribes. That is the first task. The second one is to render it practical.

Senator MASON—Yes, sure.

Mr Chadwick—That is what takes us down to these details: what can you use an e-tag for if you are going to develop tollways? What can you use a home information system for now? How does one activate a web cam externally? What are the legitimate limits on accessing a person's email account before he or she has opened their received emails? These are the issues that we are attempting to get across. You asked the question: are we busy with it? Yes, we are. Are we Solomon on these issues? No, we are not.

Senator MASON—Let me ask a question relating to this act, and I suppose it also applies more generally. Towards the end of your opening remarks you mentioned—and if I am misquoting you, please let me know—that this committee should be mindful of the distinction

between acts of surveillance on the one hand and the fruits of that surveillance on the other hand. That is the distinction that the Commonwealth legislation, the Privacy Act, makes; isn't it? In other words, it is not just about the information itself but also the use of that information.

Mr Chadwick—And it is not just about the use. If we turn not to the acts of surveillance—the actual entering of a home or whatever it is; what our law typically characterises as privacy of the body, for example, or privacy of the home, the domestic space—leaving aside acts of invasion of privacy, there is then the issue of the information derived from those acts. So, for example, in the reading of a diary or letters, or the reading of email, it is not just about the uses to which the state might put that; it is about whether the state secures it when it is in its custody and whether it is of accurate quality, especially where the state purports to take decisions adverse to the individual on the basis of that data.

Senator MASON—So you are talking about the warehousing and the auditing of information. Are those facets of your concern catered for in this legislation? Is it sufficiently comprehensive?

Mr Chadwick—It seems to me that the surveillance devices acts are not attempting to, as it were, cover every area in which the state might collect information about people. In terms of surveillance devices, one of the points I have made to the committee is the importance of approaching that in a broader fashion and, as I mentioned in my opening remarks, recognising that the bursts of law reform activity in this area tend historically to follow technological development. That is what I was drawing attention to.

Senator MASON—I suppose that is what my opening question was about. I suspect that this will be a never-ending pursuit by legislation of technology.

Mr Chadwick—Maybe that is one reason why we strive for the technology neutral approach and also that we ensure that the oversight goes along. So what happens is that you recognise the technologies are going to shift but you have at least two minds working on it, as it were: the executive mind and the judicial mind. That is putting it broadly. Sometimes we seem in this bill to uncouple the oversight from those who may be using the powers or the fruits of what is gained from such surveillance.

Senator MASON—Finally, you mentioned that surveillance can affect the watched and the watchers. Is that like a 'Big Brother' effect?

Mr Chadwick—If one looks at the literature, what one finds is that systematic surveillance can have an effect on those who conduct the surveillance. That is a general statement. I think it would be supported by the literature, and we can go into the detail if you like.

Senator MASON—I watched *Big Brother* on TV the other day, and I thought that that behaviour was perfectly natural!

CHAIR—I think the numbers speak for themselves, Senator Mason!

Mr Chadwick—If I can take you up on the term 'Big Brother', most of us of a certain age think of Orwell's novel, but you are raising it now in the context of a reality television show. I know exactly what you mean—

Senator LUDWIG—I don't.

Mr Chadwick—but the point is that one of the difficulties of discussing this issue nowadays is that 'Big Brother' used to be shorthand language for concerns about ubiquitous surveillance by the state, as evidenced by Orwell's novel. Nowadays it is a bit different. Younger people especially are much more comfortable with what others might see as technologies of surveillance—for example, cameras in mobile phones. But where the state chooses to engage in surveillance and to keep the fruits of it, or use it adversely, that always raises the concern of law. Instead of speaking in generalities, I refer to Justice Holmes in Olmstead—the US Supreme Court case—one of the great cases on wire-tapping. In his judgment in that case—I think it was in 1928—he said:

Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.

Of course, I do not mean to assert that Justice Holmes is right in the contemporary Australian context of the motives of those who seek to amend the bill; what I am doing is sounding the warning I think history has for all of us, which is that proper oversight is essential in this area.

Senator MASON—You are right. But, in closing, perhaps I could add that, in 1928, young people were not so much prey to the cult of self-expression which I suspect is one of the underlying things of our age.

Mr Chadwick—That is not what people said about the jazz craze that was around then.

Senator SCULLION—I apologise for asking questions on another submission—although I note that the New South Wales Council for Civil Liberties fairly seamlessly answered some very good questions on yours! Evidently I am operating with an antiquated hearings program. Recommendation 7 in your submission is that clause 46 should be amended to require independent oversight by the Ombudsman of any decision by police to destroy surveillance records. On the face of it, in terms of protecting privacy, that seems like a very laudable idea. But I wonder how practical that would be in terms of surveillance, intelligence gathering and investigation. You may have a surveillance device that provides certain information. You may then go on to a record of interview in which you will ask questions quite lawfully in regard to a number of issues surrounding the information you have gathered by using a surveillance device. That becomes a separate issue, because it is then part of a record of interview; it has been lawfully gathered—they have given information. That information may be part or all of the information that was obtained through the surveillance device. Under the act, this may necessarily be beyond the purview of the Ombudsman. There may be other investigations, subsequent to that information, of other persons who may provide other information. In a practical sense, it seems that it would be almost impossible to track the impact of intelligence in those sorts of circumstances. In terms of ensuring that we destroy the direct records, the impact and effect of that surveillance would be so widespread that it would not be possible to control the use of that information.

Mr Chadwick—First of all I would say that it is not a reason not to try, at least at the front end. That is a general response. I am also sure of the experience we have in Australia of trying to calibrate the balance properly. Sure, it can get hard headed but there is practical advice on how far you can go. I agree there is a limit to how far it can go with the accountability after

the uses of the powers. It does not mean that one does not start with the assumption that there will be a proper independent oversight capable of asking. My experience certainly in Victoria is that the Ombudsman in dealing with Victoria Police is perfectly capable of appropriate oversight activity. I am sure that is true at the Commonwealth level.

Senator SCULLION—To get some clarification on that, when you talk about independent oversight and actual destruction are you talking about an independent individual from the Ombudsman being present to ensure that all those things happen?

Mr Chadwick—Let us make sure we are on the same point here. In talking about independent oversight I do not just mean retention of records issues. On the retention of records issue, if you are going to have some set of rules that says material apprehended has finished its useful life—for example, material is obtained in an operation that leads in part to prosecution, the prosecution is complete, whatever it is, or there is no prosecution—and after a given time shall be destroyed, then it would be useful, given some historical examples, to have some oversight to ensure that happens.

Senator SCULLION—What sort of body do you think would be appropriate to have that oversight?

Mr Chadwick—That is a matter for others who have seen these operations and the oversight of these operations in detail. I suggest that one of the indicia of the body be that it is independent of the entity that is supposed to conduct the function. Whether that is the Ombudsman or some other accountability body is a matter for the relevant jurisdiction.

Senator SCULLION—Thank you.

CHAIR—Thank you for your time and for the Victorian Privacy Commission's submission. It has been of great assistance to the committee.

[11.31 a.m.]

BATCH, Mr David Allan, Senior Legislation Officer, Australian Federal Police

LAMMERS, Mr Rudi, Manager Technical Operations, Australian Federal Police

LAWLER, Mr John, Performing the duties of Deputy Commissioner, Australian Federal Police

CHAIR—Welcome. The AFP has lodged a submission with the committee, which we have numbered 5. Do you need to make any amendments or alterations to that submission?

Mr Lawler—No, we do not.

CHAIR—Deputy Commissioner, would you like to make an opening statement, and then we will go to questions from members of the committee?

Mr Lawler—Thank you. The AFP appreciates the opportunity to give evidence in relation to the proposed provisions of the Surveillance Devices Bill 2004. Before I start, I would like to firstly give my apologies for Commissioner Keelty, who was to attend this hearing this morning but has been called away on duties relating to the National Security Committee of cabinet. He offers apologies and was intending to appear.

CHAIR—Please thank the Commissioner for us.

Mr Lawler—The AFP works closely with other Australian and international law enforcement bodies to enhance safety and security in Australia and to provide a secure regional and global environment. Globalisation of crime has resulted in an increasing Commonwealth requirement to deal with terrorism, organised crime, money laundering, major fraud, illicit drug trafficking, people-smuggling and trafficking and e-crime. The provisions proposed in the Surveillance Devices Bill are essential in ensuring that law enforcement can effectively investigate transnational offences and keep pace with suspected criminals, who increasingly use advanced technologies and counter-surveillance techniques to evade law enforcement detection. The Surveillance Devices Bill seeks to consolidate and update the regulatory regime for the use of surveillance devices by Commonwealth agencies and bring those agencies into the 21st century.

The bill is broadly based on the model surveillance devices legislation developed by the joint working group on national investigation powers with some necessary adaptations for the Commonwealth jurisdiction. The bill establishes a structured process for law enforcement use of surveillance devices in areas where there is currently no structured process. It is proposed that the AFP may use surveillance devices for the investigation of Commonwealth offences which, in the main, carry a penalty of at least three years imprisonment or to assist the recovery of a child where the Family Court of Australia has issued a recovery order. The AFP may also use them to investigate a state offence which has a federal aspect that meets the three-year threshold.

If I may, I would like to draw the committee's attention to the fact that, under the provisions of the bill, the AFP may only use surveillance devices without permission on private property or in a vehicle by way of a warrant issued by judge or an AAT member,

unless special circumstances of urgency exist that involve serious risk to a person or property, urgent circumstances relating to the recovery of a child or where there is risk of the loss of evidence for certain listed offences such as terrorism, drug offences, espionage, sexual servitude and aggravated people-smuggling. It is the view of the AFP that the provision for emergency authorisation relating to loss of evidence should be extended to child sex tourism offences, given the gravity and nature of these crimes.

With regard to accountability, the proposed regime imposes significant and potentially onerous reporting measures that apply in addition to the AFP's existing accountabilities. These existing accountabilities include the AFP's professional standards regime and Ombudsman's oversight, and there is always the discretion of a court to exclude evidence obtained from surveillance devices if it is found to be irrelevant or to have been obtained unlawfully or inappropriately.

Whilst the AFP will monitor the reporting requirements and their effects on our capacities, we acknowledge the need to balance law enforcement and privacy considerations. The AFP considers that surveillance is a crucial tool for effective and efficient law enforcement. From a law enforcement perspective, the bill will support increasing effectiveness with respect to all types of criminal activity, including terrorism. The advent of comprehensive surveillance device legislation modernises and clarifies surveillance device powers that can be used by Commonwealth law enforcement agencies. The Commonwealth legislation will complement intrajurisdictional and cross-border surveillance device initiatives being developed by the states and territories under the auspices of the Standing Committee of Attorneys-General and Australian Police Ministers Council. The AFP supports the bill. That is my opening statement on behalf of the AFP.

CHAIR—Thank you. I will go to your suggestion that the AFP supports the extension of these powers to the investigation of child sex tourism offences. Has the AFP put that to government and, if so, what has been the response?

Mr Lawler—I understand that there have been discussions in relation to extending that power. The question of the exact status of that suggested amendment might be better addressed to the Attorney-General's Department, but certainly it has been put forward.

CHAIR—We will have that opportunity, so I am sure we can follow that up. There was a suggestion in evidence this morning that this would be more effective legislation if it were technology neutral—that is, if it took greater effort to not tie itself down to what we now use and was perhaps cast in more technology neutral terms. I think it was the suggestion of Privacy Victoria in particular. Do the AFP have a view on that? Does the casting of the legislation constrain you operationally because of that?

Mr Lawler—I will start in relation to the specific question. My understanding is that the definitions contained within the bill are sufficiently broad to capture the sorts of base technologies that we are talking about. Of course, we do not have a crystal ball to predict where technology might take us in the future and, as a result of this bill being brought forward, we quite clearly have a capacity to catch up on technologies that the legislation has lagged behind on. Having said that, as it stands it would seem as though there is a capacity in

the known technologies as they present themselves for the bill to capture advances in the future.

Mr Batch—Under the definition of surveillance devices there is a provision that allows a device of a kind prescribed by the regulations, so there will be flexibility if there is something that has not been anticipated under the current provisions.

CHAIR—The committee has had some discussions this morning about the difference between some of the provisions of this bill, particularly the checks and balances, and those contained in bills such as the Telecommunications (Interception) Act 1979. One of those is that, as I understand it, applications made under the T(I) Act for a warrant have to be supported by an affidavit, no matter the context, whereas this bill suggests that in an emergency situation there would be no requirement for an affidavit. From the AFP's perspective is there an operational reason why that would be the case, or would it be equally possible to do it in both circumstances?

Mr Lawler—If I can, I might like to come back and talk more broadly about the different levels of what is proposed under the bill, but my understanding in relation to emergency authorisations is that an affidavit would be presented to an authorising officer—be that a judicial officer, a judge or a member of the Administrative Appeals Tribunal—up to two working days after an emergency authorisation had been approved. My understanding is that there would be a formal affidavit prepared.

CHAIR—The turnaround in the T(I) Act is 24 hours, isn't it?

Mr Batch—I would have to take that on notice. I am not entirely sure.

CHAIR—We are all working without a T(I) Act in front of us, which is not entirely helpful. If it were the case that there was a 24-hour turnaround in the T(I) Act, would it be operationally difficult to administer if it were the same for the Surveillance Devices Bill?

Mr Lawler—In the context of the Surveillance Devices Bill, certainly the difference between telephone intercept and the sorts of technologies that are being applied here in an operational context means that the deployment of the equipment is much more immediate. So the opportunity and the circumstances as presented, given the nature of the technologies we are talking about, are very different. I could talk about that further if you would like me to.

CHAIR—Mr Lawler, in your opening statement you referred to the safeguards in place for providing emergency authorisations and said that one of those was the possibility of exclusion of evidence if the authorisation approval is then not received when it goes before the appropriate judicial officer. What do you say to the suggestion that evidence or material that is obtained under the surveillance warrant before approval is declined should be destroyed, because the bill does not currently provide that?

Mr Lawler—Can I just clarify a point in your question. I was referring to the ultimate discretion of a court. I was raising the fact that, even if in an emergency situation a judge of the AAT ruled that an authorisation was appropriately granted and then subsequently granted the authorisation, and hence the admissibility of the evidence, subsequently in any court proceedings that information and evidence could still be excluded if it were determined on all the facts, as presented by both the prosecution and the defence, that either it has been

inappropriately obtained or its probative value outweighs its prejudicial nature. So there is actually another check and balance after the approval process.

Where the application is declined in those instances, there may be a very good reason for the commissioner to retain that material. It may well be that the particular officer involved has acted inappropriately and that that material would be required to mount a successful prosecution of that official in those circumstances. It may well be that there are broader implications and other circumstances involved where that information and evidence would be relied upon for those sorts of prosecutions. So it is a safeguard to enable the proper application of the law, and it is an accountability regime to ensure that those persons who might be so minded to act outside the accountability regimes in place can be brought before appropriate authorities.

CHAIR—But there may also be a circumstance where the surveillance and the material obtained through that surveillance has been done unlawfully and inappropriately. Where are the protections for the person who is unlawfully surveilled?

Mr Lawler—That is true and that is acknowledged, but to balance off against that potential inevitability are a strict array of regimes that relate, talking about the Federal Police, to criminal sanctions in relation to the management, disclosure and control of that information under the Australian Federal Police Act. In addition, I understand there are significant constraints and penalties in the context of this act, so not only in the context of this act but more broadly in relation to the Australian Federal Police Act.

Senator LUDWIG—Privacy concerns are an issue that has come up from a number of submitters. Under the telecommunications interception legislation, when applying for a warrant privacy issues are canvassed. They are not so under this bill. Why the difference? Would you not consider them in any event?

Mr Lawler—I might talk broadly about that and make some initial comments that the nature of the technologies and the intrusive nature of what is proposed in the bill is on a graduated scale here. The telephone interception capacities and the intrusive nature of those capacities should not be, I do not think—certainly this is the AFP's view—aligned with all the capacities that are being discussed under this particular bill. Their level of intrusiveness and their application are very different. If I can use the ends of the spectrum, there are telephone intercepts at one end and at the other end the use of binoculars in a public area. Quite clearly the level of intrusiveness is very different.

There is also the use of an opening device in a package that has been seized and found to contain narcotics. One can capture the spoken word in quite an intrusive way in the personal communications of members of the community as distinct from using an opening device in a package that has been seized by Customs officials and found to contain heroin. In that context the purpose of the opening device, which is captured under the surveillance devices legislation, when a substitution has been undertaken and the package put back into the mail system, is to allow law enforcement officers the capacity to know when the package has been opened. That is the extent of the intrusion. So you can see that the nature of the application and the types of devices are very different. But to ask for both to have the same level of accountability I do not think is justified. The reality is that it would cause significant

operational impediment for the AFP because what is required to actually prepare the affidavits and prepare those accountabilities causes significant capacities to be applied by the Federal Police.

Senator LUDWIG—Perhaps you can provide some comment on this and I will share my difficulty on some of these provisions with you. The range you speak of is quite broad, but let us take the range of optical surveillance. The range can be, as you have said, I can observe you and you can observe me, I can use binoculars, a telescope or infra-red tracking, sophisticated satellite—I can use a whole raft of things that I probably do not even know about—

Mr Lawler—Possibly I don't.

Senator LUDWIG—which are at the higher end and which at least to me are significantly intrusive, if you are using infra-red and those types of surveillance devices. At the binoculars level in a public place, granted, there may not be a requirement because it seems to go on undisturbed anyway, but at that higher end it seems to me that it is very intrusive and you do collect a significant amount of information because it can be captured and recorded and then there is the retention of that captured and recorded material, how it is stored and utilised and how it is maintained over time. I am unsure about that and I am unsure whether that should be subject to a warrantless position, so described in this bill.

Mr Lawler—The AFP's position respectfully is that it should not be. I understand your point exactly, and it is valid to a degree. From our perspective, what is occurring in the context of normal surveillance—person-to-person—is that with enough surveillance capacity it can be achieved. For example, if we were to take the use of infra-red—and I will not make specific comments about that in this forum outside of in camera—and surveillance were to be undertaken at night, the same result could be achieved but with just more resource, more people to undertake the activity. Ultimately, in a theoretical sense, an outcome could be achieved in the context of using people. The technology allows us to be more efficient and to make sure that the capacities and resources that we have been given are most effectively applied to a particular situation.

Senator LUDWIG—I do not want to labour the point, but what about at the higher end which does not require warrants, such as optical, that could not be dealt with by the use of extra resources such as using significant listening devices which can hear a pin drop 30 yards away? In other words, you can penetrate a house, which could not otherwise be listened to, by as many agents as you can find a keyhole to put their ear to or by using heat sensing cameras that can then track body movements and people in houses. That could not be done unless you had a number of keyholes in every door. Those sorts of technologies could not be dealt with in any other way. You would not be able to do it. In this bill you are seeking a warrantless ability to be able to do it with significantly fewer accountability requirements than, say, the TI legislation. I am grappling with why. Why should you have it without those accountability mechanisms? Why should you be able to use those devices without a warrant?

Mr Lawler—I wish we had those technologies. Having said that, there are accountabilities with or without a warrant in those circumstances. Let us take the optical surveillance example that you articulated, which is through an internal authorisation process. It is a process that has

been previously endorsed in the context of controlled operations. This is not a new process; this is a process that we say is applicable to the level and nature of the device that is going to be deployed. As you know from previous discussions, the use, management and control of controlled operations has been successfully employed. It is that level of accountability and that mechanism which will be utilised in areas—not at the bottom end of the spectrum nor at the top—that fall within the middle range as being an appropriate response.

Senator LUDWIG—You diverge from the joint working group in some matters, and I think they are articulated in your submission. I will not read them in total, but there are four dash points which go to internal authorisation for tracking devices where there is no entry onto premises and interference with the interior vehicle without permission. They also extend to power to use optical surveillance devices without a warrant, the availability of emergency authorisations for risk of losing evidence in certain serious offences and extraterritorial application of warrants. Those were the additional matters amongst maybe some other minor issues that were departed from in relation to the joint working group. Where was the impetus from? Where did those issues come from? They did not come out of thin air, I suspect.

Mr Lawler—No, those issues came from the AFP and were based on our operational considerations and the fact that the model working group was particularly focused on cross-border application of surveillance devices. The nature of the AFP's business in Commonwealth jurisdiction is very different. Whilst we have in large part adopted the model surveillance devices legislation, the nature of the committee's work did not specifically focus on the unique nature of the AFP's business. That can be starkly seen in the context of our international work—something that did not have to be and was not necessarily focused on by the committee, which was looking at the application across state borders.

To go to some of the other issues, the nature of the AFP's business, particularly in the context of the work we do at the border—especially with narcotics and paedophile material, false documents and other contraband—means that these sorts of technologies are very frequently employed. They are employed in a number of contexts: in gathering evidence and in ensuring safety and security when we are conducting controlled operations so that we can provide an undertaking to the community that we can actually protect the narcotics that we might subsequently be allowing to move forward into the community in a controlled environment. So these are standard tools of trade. They are fundamental to the work of a sophisticated Commonwealth law enforcement agency and set us apart from the nature of the work that is being undertaken by state and territory jurisdictions predominantly.

Senator LUDWIG—Should the parliament pass this bill, do you expect to get it 100 per cent right every time in the use of those powers or do you expect that sometimes you might make a mistake in the application of those powers?

Mr Lawler—I am sorry, but I did not quite understand that question.

Senator LUDWIG—In the use of the power that is provided for in the bill, should that bill pass, do you expect that you will get that right 100 per cent—that you will use it appropriately and correctly every time?

Mr Lawler—I am certainly an optimist. We have very strong corporate governance regimes in the AFP. I think that has been demonstrated time and time again. Having said that,

I am also a realist and I understand that we are dealing with people that are subject to human frailties. In that context, and acknowledging that that is a fact with human beings—police officers are included quite clearly in that category—we need to then have mechanisms in place to treat that risk in a way that is acceptable to the community on balance. Some of those treatments are in the context of a very rigorous professional standards regime, a very well-received and adopted confidante reporting program, Ombudsman oversight and strict management oversight and reporting. So there are different layers, levels and facets of control and management of the powers that the AFP has already and also of the powers that are proposed. Some of these powers and activities are already being employed by the AFP. It is just that there is no clarity and mechanism surrounding what is there at the moment.

Senator LUDWIG—The use of a civil remedy regime similar to the TI legislation would not concern you then, if it were included in this bill?

Mr Lawler—I was briefed outside the meeting on questions of that nature and I do not profess to have the expertise in relation to the civil applications and civil remedies that might be available. I think that is best left to others that are more conversant with the law in respect of that. But certainly my understanding is that, if one were to have acted inappropriately, then one would expect all the accountabilities and remedies to be available.

Senator LUDWIG—With regard to the keeping of records, there has been evidence today that the bill lacks in part a sufficiently accountable process to ensure that records that are no longer required are appropriately dealt with or destroyed, as the case may be. How do you keep your records in relation to these processes—or how will you keep them?

Mr Lawler—The AFP is well versed in the management of records, particularly in the context of the application of the Telecommunications Interception Act. It is an organisation that is dealing with the top end of documents that are sensitive and, by their very nature, need protection. So there is a culture in the organisation of the protection of documents, of the security of documents and of the need to know principle. The issues of unlawful disclosure of information and the improper use of information are things that we are very active on. That is borne out by a number of proactive investigations that have identified people in our organisation who, unfortunately, may have acted inappropriately. The number of these people is very small; however, we have been able to identify them and to make sure that the organisation as a whole is very aware of their responsibilities.

Apart from the comments that I made at the start about the volume of material, particularly reporting post the application of devices and instruments that are covered in the Surveillance Devices Bill, I do not see any difficulty in the process, the mechanism, the culture of storage or the reporting and recording of those. But I think the issue of volume will be a significant concern for the organisation. I think the number of applications, both internal and external, will make it such that that will be very onerous. We will commission over time some studies about the capacities of the organisation that go to meeting these reporting regimes, because we are concerned about that.

Senator LUDWIG—And the only way to limit that of course is to have an effective destruction process that also sees that the records are destroyed appropriately. You would not object to any process that assisted in that, would you?

Mr Lawler—We are very keen. We have no desire to retain records any longer than is absolutely necessary. So we are very supportive. We do maintain a rigorous regime of destruction under the telephone intercept provisions, but of course there are specifics in this particular bill that give an opportunity to make sure that justice is properly applied.

Senator SCULLION—I have a couple of supplementary questions, just for the edification of the committee. Perhaps we watch too much late night TV, but technology rolls along and, quite honestly, it is very hard as a member of the public to validate what is fantasy and what is reality—it all seems to blend. Could you on notice provide us with a list of those surveillance devices that you consider would not require a warrant and processes? I do not need something too comprehensive. But, at the moment, watching someone with a pair of binoculars is as far as I would understand it would go—but, from discussions, obviously it is not. If you could provide that on notice, I would appreciate it.

In response to a question from Senator Payne with regard to the capacity for the evidence that was taken then not authorised, you responded by saying that you might need to hang on to it. When asked why you wouldn't support the judge determining that it not only was inadmissible but also should be destroyed, you said, 'We may need to prosecute those involved.' I understand and accept that, but the NSW Council for Civil Liberties has put that it is not actually an offence to obtain the information.

In section 45, which I have just had a comprehensive look at, there are penalties of two and 10 years respectively for the use, recording, communication of the information—what you actually do with the information—but it does not appear to be a specific offence to procure that information without any of the audits that we have spoken about with respect to the AAT, an internal review or the judicial system. When you said that you would be able to take action against any officer—and I am assuming in all different departments—under what legislation would you take action against an officer who did not act lawfully with regard to the getting of information rather than the distribution of it?

Mr Lawler—My understanding is that the offences that are brought to bear in those sorts of circumstances are in fact state offences—that is, for the gathering of that information unlawfully. David may be able to add some further clarification.

Senator SCULLION—You can take it on notice.

Mr Lawler—We are happy to answer it now.

Mr Batch—If an authorisation is subsequently disallowed, the collection of that evidence in the period from when the authorisation was given to when it was disallowed is not unlawful. There is an express provision in the legislation that limits the use of that information—it cannot be used in a criminal proceeding, which is why it is inadmissible—but the evidence collected in that time in itself will not be unlawful.

Senator SCULLION—I understand that. What I was going to was an extension of that thought process. We talk about the use of the evidence. What about the bright young police officer who says, 'I'll just go and grab that camera off Joey before he puts it back and I'll just go in and bug the bag in the house and stick a few cameras in. I know I'm not allowed to, but I'm keen and zealous'? This particular legislation does not provide that that is an offence. This legislation provides for the use of the information that one gets—lawfully, it is assumed,

even if it is something that is subsequently found to be unauthorised—and it deals substantively with that. However, this bill does not appear to deal with the issue of not having the appropriate authorisation to take information through various surveillance devices.

Mr Batch—If someone was to enter a private premises without an appropriate warrant, there would be relevant state property offences attached to that.

Senator SCULLION—So your response is that this is covered under state and territory legislation?

Mr Batch—It would depend on the nature of the circumstances put before us. In that particular instance, yes, if somebody did go onto premises without the appropriate warrant or authorisation, whatever the case may be, there would be property offences attached to that. It would be, potentially, a state break-and-enter offence.

Senator SCULLION—Because we are dealing with a number of Commonwealth authorities—and I have little understanding of the differences between the legislation in the states and territories and the Commonwealth legislation—wouldn't it be reasonable, as we are dealing in such detail with these issues, to put up front in the legislation that it is an offence and prescribe penalties for acting outside of the authorisations processes that are put in place? Why rely on state and territory legislation when it is such an important part of a piece of legislation we are putting together?

Mr Batch—The Attorney-General's Department might have a broader criminal law policy position on why they have not dealt with that specifically in this bill.

Senator SCULLION—Thank you very much.

CHAIR—Thank you very much, Deputy Commissioner, Mr Lammers and Mr Batch, for assisting the committee. If there are any issues the committee wishes to pursue through questions on notice we will do that as speedily as we can. The reporting date for the inquiry is 27 May, so it is not quite as pressing a turnaround as it has been in recent times for responses to questions. Thank you very much.

[12.09 p.m.]

JACKSON, Ms Maggie, Special Adviser, Criminal Justice and Security Group, Attorney-General's Department

SMITH, Mr Nick, Senior Legal Officer, Security Law Branch, Attorney-General's Department

CHAIR—Welcome. The department has not formally made a submission, but before we commence may I remind senators that, under the Senate's procedures for the protection of witnesses, departmental representatives should not be asked for opinions on matters of policy. If necessary, they must also be given the opportunity to refer those matters to the appropriate minister. Ms Jackson, do you wish to make an opening statement?

Ms Jackson—Would it be helpful to the committee if I were to try to introduce some transparency into the match between state and Commonwealth legislation and the model that was developed by the joint working group?

CHAIR—Let's start with that, and then we might go to some questions.

Ms Jackson—Unlike in relation to telephone intercept, the Commonwealth does not have any constitutional power over surveillance devices per se, and that necessitates the very narrow focus that the legislation has on the activities of the AFP and the ACC. The model legislation was developed following the leaders summit to enable state and territory police to conduct cross-border investigations. This legislation is intended to provide a regime whereby police in one jurisdiction could gain authority in that jurisdiction to act in other jurisdictions in a lawful way, and their activities there would be recognised as lawful in all Australian jurisdictions. That was the purpose of the joint working group exercise. It was made clear at the outset that some states were proposing to use this as a model for their intrastate surveillance as well. Other jurisdictions said that they preferred the different regime that they had for intrastate and would be retaining two separate regimes.

The Commonwealth currently has legislation that deals only with listening devices—in the Australian Federal Police Act and in the Customs Act. There is no more general surveillance power, although the Commonwealth is exempt from some of the state regimes. This is a fairly unsatisfactory position and the Commonwealth has sought, in seeking to achieve a greater measure of uniformity than currently exists, to work with the model legislation to develop something that would be suitable for Commonwealth investigative regimes.

Some of the submissions that the committee has received urge a situation where there is judicial oversight of the warranting processes. The committee might recall the difficulties that arose in the case of Grollo for warrants that were issued by federal judges that would then be reviewing the operation of the warrant and so on under the Administrative Decisions (Judicial Review) Act. Amendments were then made to the TI act because federal judges were, by and large, no longer making themselves available to issue warrants. As a consequence of that decision, we authorised Family Court judges and AAT members to issue warrants. For us, the situation is complicated by having a small pool of judges who have the function of conducting reviews of administrative decisions and can also in certain circumstances be brought into the

criminal justice process and adjudicate on the warrants that they themselves have issued. The process of using the AAT was developed to overcome that perceived conflict of interest and the unavailability of most Federal Court judges to issue the warrants.

A number of submissions also urged a greater measure of parliamentary oversight of this regime. There is already parliamentary oversight provided by the ombudsman reporting to the minister and the minister tabling the ombudsman's reports in the parliament. There is also a provision in clause 50 of the bill which requires the agencies to report annually to the minister, and those reports will also be tabled.

In relation to the safe storage of the material, there are provisions in the bill that deal with the storage of the material by, in clause 46, the agencies themselves and, in clause 48, the courts and the AAT. There was a lot of discussion about the records of destruction of information under the bill. Clause 46 requires the chief officer of an agency to destroy material that is no longer relevant, and clause 52(j) requires them to make a record of the fact that information has been destroyed so that that record is available to the Ombudsman and he can include that material in his audit.

There was a fair bit of discussion this morning about emergency authorisations. In fact, the telephone intercept regime does provide a regime whereby one can do warrantless interception for 24 hours in certain limited, urgent situations and then go and obtain a warrant through the mechanisms of that legislation. In that sense, the bill is not dramatically different. There was also some discussion about whether affidavits are required to be made for emergency authorisations. While they are not required for the actual emergency authorisation itself, one goes to the court or the AAT to have that emergency authorisation approved, and clause 33(2)(b) requires an affidavit to be provided. So there seems to be a little confusion about that.

In terms of the warrantless use of surveillance devices, there were assertions that no accountability at all attaches to some of those situations. In fact, paragraphs 52(e) and 52(f) require the agency to record all uses of surveillance devices, not simply those which are conducted under warrant. So there are mechanisms for recording and for the Ombudsman's oversight of those activities. Some of the discussion this morning also concerned the consideration of privacy issues when one is considering applications for warrants. The legislation in paragraph 16(2)(c) specifically requires the court to consider the privacy implications of granting a warrant before it actually approves the granting of a warrant. While privacy concerns are not addressed in the objects clause, they are clearly required to be taken into account before a warrant is issued. There are no other specific issues that I want to address before we go to general questions.

CHAIR—Mr Smith, do you wish to add anything?

Mr Smith—No, thank you.

CHAIR—Ms Jackson, you referred to the discussion we had about emergency authorisations and the differences between this and the application of a similar process under the TI Act. As I understand it, this bill says in subclause 33(1) that the application to the judge or nominated AAT member for approval of the giving of the emergency authorisation has to be made within two business days after providing it.

Ms Jackson—Yes.

CHAIR—Would I be right in then saying that, if an emergency authorisation is provided by a police commissioner or someone on a Friday afternoon, reference does not have to be made to the court or the AAT until the Tuesday afternoon, so a surveillance device could be used for four consecutive days before any application is made to the court?

Ms Jackson—Yes.

CHAIR—Why is it two business days and not 48 hours?

Ms Jackson—That is also based on the joint working group model. I do not actually recall the discussion at the joint working group about that time period. It may well be based on some of the state legislation, but it is already in the joint working group model as two business days.

CHAIR—Is it a usual authority provided under this sort of legislation that surveillance or an intercept could be carried on for four days without a warrant before any application to the court is made?

Ms Jackson—It is true that in the TI act it is 24 hours, one day.

CHAIR—We might have a look at the joint working group model, as you suggest. I think you probably heard Acting Deputy Commissioner Lawler refer to the AFP's interest in having the legislation extended to cover child sex tourism offences. Does the department have a response on that issue?

Ms Jackson—That is really not an issue that we have yet had an opportunity to raise with ministers. It was raised with us recently.

Mr Smith—Certainly you can get an SD warrant for child sex tourism offences. I think what he is referring to is extending the emergency authorisation provisions on loss of evidence. We have not considered that one yet.

CHAIR—I see. I have a question about this bill's overlap with the TI act. In the TI act there is a formal civil remedy process, in section 107A, for unlawful interception or communication. This is not replicated in this proposed act. What is the reason for the difference between the two?

Ms Jackson—It is partly because of the complexity of the match between Commonwealth and state laws here. Given that we have no power directly over surveillance devices, we have not made the use of any of these devices unlawful. We are totally reliant, as Mr Batch told the committee, on state laws to prohibit the use of them. Therefore, while we provide a regime that authorises law enforcement use, the fact that it falls outside that regime, particularly as to the optical surveillance device area, does not mean that it is necessarily unlawful in the jurisdiction in which it occurred. To have a provision that said 'any surveillance device that is used other than in accordance with this act' might expose a Commonwealth law enforcement officer to a regime that was different from that of a state law enforcement officer or a private citizen operating in that same jurisdiction. It is a complex match of the Commonwealth and state laws that is really underlying the issue there.

CHAIR—Are you confident that, without a regime being incorporated into the proposed act, there is adequate protection for Australian citizens who may be subject to unlawful surveillance under activities carried out under this bill?

Ms Jackson—You have the complaints against police legislation and you have the provisions of this bill that prohibit the use of unlawfully obtained material, including material that was obtained under an emergency authorisation that is not subsequently approved in the use of any criminal proceedings. That is specifically provided for in the legislation. I think the AFP was perhaps a little less clear on that issue. It is not a question of reliance on the Evidence Act; this bill specifically says that information cannot be used in criminal proceedings.

CHAIR—If material were obtained under an emergency authorisation which was subsequently not approved, could it then be used by law enforcement agencies to pursue other prosecutions, other issues, for another investigation?

Ms Jackson—Yes.

Mr Smith—Not for the investigation of a suspect—of a police officer, certainly. Section 45(6) is the provision which governs the more restricted range of exceptions which apply to that sort of material, and it excludes 45(5)(a), (b) and (c), which are the investigation of a relevant offence, the making of a decision regarding a relevant offence, and so on. The police investigating other offences are excluded from the use of that kind of information. They could, of course, still bring an investigation under the Privacy Act or the Ombudsman Act against the police officer, but not with regard to an offence of a suspect.

CHAIR—No; it is the use of the material in regard to a suspect that I am concerned about, in this case.

Senator LUDWIG—So there is no derivative use—

Mr Smith—It can go to ASIO or the intelligence agencies but it cannot go within law enforcement for law enforcement purposes.

Senator LUDWIG—But that information can then aid the subsequent investigation of an investigation by the AFP, if it so desires.

Mr Smith—If the AFP were prosecuting one of its own, for example, yes, it can be part of that criminal investigation.

Senator LUDWIG—The destruction of records has been raised, from recollection, by a couple of submitters. The regime that is contemplated under this bill seems to—unless you can take me to the provision—fall short of what is under the TI act. Or do you say it is the same?

Mr Smith—In what sense? Provision 46 was modelled quite closely on the TI act provision that as soon as the chief officer—or his delegate, in this case—is satisfied that the piece of material is no longer relevant to the permitted purpose it must be destroyed, and the Ombudsman is entitled to look at the chief officer's satisfaction of that fact.

Senator LUDWIG—And you say that is similar to the TI act.

Mr Smith—As I recall, we modelled this provision on the TI act.

Senator LUDWIG—If that is different, perhaps you could advise the committee.

Mr Smith—I will have a look at that.

Senator LUDWIG—Is that similar to what was proposed under the joint working group?

Mr Smith—As I recall, we moved away from the model working group, more towards the TI model.

Senator LUDWIG—What did the joint working group propose?

Mr Smith—That might have been modelled on the TI act as well.

CHAIR—It sounds like you have gone in a circle, then.

Senator LUDWIG—I am happy for you to come back on that issue and inform the committee if there is any departure from what we have been discussing. The use of the TI act also requires reporting to parliament on the use of the power. This bill does not seem to contemplate, other than by report to the minister, the use of the power and then, of course, the oversight by the Ombudsman. Is there any reason why you would not include a provision that allows parliamentary oversight similar to the TI legislation?

Mr Smith—The chief officer must file a report every year to the minister—

Senator LUDWIG—Yes; it is to the minister, though. The minister does not have to then make it available to parliament.

Ms Jackson—He does.

Mr Smith—Subclause 50(4) states:

The minister must cause a copy of the report to be laid before each house of parliament within 15 sitting days after he receives it.

Senator LUDWIG—Is that similar to the TI legislation?

Mr Smith—I believe so.

Ms Jackson—That is clause 50, subclause (4).

Mr Smith—The relevant part of the TI act is section 93.

Senator LUDWIG—Yes. The report has to be laid before parliament. The information to the minister includes information on each warrant or authorisation. What about those that are warrantless and those in emergency circumstances that were refused? What happens to the advice to the minister, or that which parliament may otherwise be able to understand, in the two instances—those that are warrantless and those that are an emergency but where no warrant was granted?

Mr Smith—When you say 'warrantless', do you mean tracking device authorisations or—

Senator LUDWIG—And optical surveillance.

Mr Smith—Which is completely outside the paper trail.

Ms Jackson—Tracking device applications are covered.

Senator LUDWIG—The relevant agency is required to keep a record of the use of tracking devices and optical surveillance, so there is a record that can be overseen by the Ombudsman.

Mr Smith—Under paragraph 50(i)(e) you have to report on the number of applications for warrants, emergency authorisations or tracking device authorisations that were refused during that year and the reasons for refusal.

Senator LUDWIG—Is that report then laid before parliament?

Mr Smith—Yes. But there is no reporting to parliament purely in warrantless instances—for example, observation by police with binoculars from a police car.

Senator LUDWIG—That range can include cameras, infra-red or that sort of technology?

Mr Smith—Infra-red is difficult. I am aware that the Victorian police—

Senator LUDWIG—I do not know whether they use it.

Mr Smith—I am not aware whether they do either.

Senator LUDWIG—I guess they might after we have been talking about it!

CHAIR—They are probably eternally grateful for your suggestions, Senator Ludwig.

Senator LUDWIG—There is no reporting in relation to the use of infra-red?

Mr Smith—Purely on warrantless optical surveillance devices.

Senator LUDWIG—What about computer data, where you might have keystroke software, or remote computer data, being retrieved from a system?

Mr Smith—Insofar as it relates to the use of a data surveillance device, which is the only provision in the bill, that that has to be reported on as well.

Senator LUDWIG—That falls under the annual report.

Mr Smith—You can only use a data surveillance device under a warrant and you have to report everything but a warrant under this provision.

Senator LUDWIG—This was not supposed to be a uniform code, was it?

Ms Jackson—The Commonwealth legislation was not part of the uniform code, no. We do not have cross-border issues in the way that the states have.

Senator LUDWIG—You do not have the power.

Ms Jackson—The state law confers both power to obtain warrants to use in another jurisdiction and a mutual recognition component of warrants issued elsewhere. The Commonwealth is not required to be part of that mix. We do not physically have any territory on which they may wish to operate.

Senator LUDWIG—Perhaps Jervis Bay. We heard some evidence today from the Privacy Commission, and we will follow that up for sure. But it seems to me that the Victorian bill is now moving away from the model and it is picking up a number of matters that have been raised or that have been identified in this bill and others perhaps. Is it the view of the Commonwealth that the states should implement similar legislation to the Surveillance

Devices Bill 2004 or that they should implement whatever they want to implement and that the inconsistencies between the two do not pose any operational difficulties?

Ms Jackson—They do not pose any difficulties for the Commonwealth, but the difficulty for a state that departs significantly from the model is whether its laws will be recognised by the other jurisdictions for the purposes of the mutual recognition regime.

Senator LUDWIG—Perhaps you could explain the mutual recognition regime.

Ms Jackson—The model bill contains provisions for obtaining warrants and using surveillance devices in other jurisdictions. The bill provides that, where there is a law of a corresponding jurisdiction—one that is similar—activities that are authorised under a warrant issued under the corresponding law can be carried out within their physical territory. So, unless the states are prepared to recognise the laws as corresponding laws, there will not be recognition of those warrants for police to enter the jurisdiction that does not recognise them.

Senator LUDWIG—It could also put them in some invidious circumstances if they extend to some of the powers that are proposed in this bill, as distinct from those in the working group. If the other states adhere more closely to the model then there are some gaps that might pose some operational difficulties, for argument's sake.

Ms Jackson—I was not aware that Victoria was adopting some of the provisions from the Commonwealth bill—

Senator LUDWIG—I think that is what they said.

Ms Jackson—but I think Victoria was a jurisdiction in which they were trying to meld their domestic intrastate regime with the interstate regime. Maybe they are moving towards the Commonwealth model for their domestic intrastate investigations rather than for the cross-border part of the regime.

Senator LUDWIG—It becomes a bit of a minefield, doesn't it. The bill contemplates that AFP employees and Australian Crime Commission staff will be able to apply for a surveillance device warrant. Why so broad when the T(I) Act confines it a little more—or am I wrong in that?

Mr Smith—With regard to the AFP, the person who applies must be a member of the AFP—that is, basically, a sworn officer. In the case of the ACC, it is any ACC employee. I believe the reason for that is that the definition of an ACC employee is fairly complex because it has to accommodate both permanent employees of the ACC and seconded officers from a range of jurisdictions, so we have allowed for the full range of ACC employees. As was raised by somebody this morning, that theoretically means that secretarial staff could apply. But I am sure that would not happen in practice, and it would not be practical to then say 'any ACC employee, except secretarial staff'.

Senator LUDWIG—We have also heard from the ACC that, in practice, they use seconded officers from other jurisdictions to exercise the power, so in fact they do not seem to need the power.

Mr Smith—The ACC will have an better explanation of ACC affairs than I have, but the ACC have a choice of exercising Commonwealth or state powers in order to fulfil their

functions. They do currently use state powers to some degree, but obviously state boundaries would be a problem with that.

Senator LUDWIG—The definition in section 5 says:

AFP employee has the same meaning as in the *Australian Federal Police Act* ...

Do you say that that only relates to agents—that is, sworn law enforcement officers?

Mr Smith—Clause 6 of the bill says:

law enforcement officer means:

(a) in relation to the Australian Federal Police—the Commissioner of Police, a Deputy Commissioner of Police—

and you are right—

any AFP employee ...

Yes, I assume that would include civilian employees as well.

Senator LUDWIG—So why so broad?

Mr Smith—I assume that would have been at the request of the AFP in recognition of who actually does that kind of work.

CHAIR—We might follow that up with the AFP on notice.

Mr Smith—Yes.

Senator LUDWIG—But you still must have conceded that and included it. I was wondering on what basis they persuaded you to adopt such a broad definition. Perhaps you could take that on notice and look at it.

CHAIR—We will also follow it up with the AFP, Senator Ludwig.

Senator LUDWIG—Thank you.

Senator SCULLION—Thank you, Ms Jackson, for your explanation on the states and territories and the jurisdictional issues in the Constitution. I appreciated that. There are specific provisions in section 42 and 43 that deal with ships, aeroplanes and that sort of stuff. I am particularly interested in the foreign fishing arrangements and how this may affect them. The issue that I am concerned about is not so much that the act seems to be silent on it but that it deals very specifically with the capacity not to need the consent of a foreign official if the vessel is in Australian waters, within our fishing zone. It deals specifically with extraterritorial surveillance—in other words, the assumption that if they are in somebody else's waters we would require the consent of an appropriate official. But one would have thought that, in the context of protecting Australian fishing zones, the necessity for prevention would be collecting information and intelligence, perhaps radio signals, Inmarsat-C and those sorts of things, prior to that.

Whilst it seems silent on these issues perhaps you could indicate to me how this would work in a high-seas circumstance. Is that considered extraterritorial or not? For example, it says that we need the authorisation of an officer from that country. As you would remember with the *Viarsa*, Uruguay was very reluctant during that process to accept that it had any responsibility, and we know that is going to be the case. If that were the case and it was

considered extraterritorial, any evidence that was gathered in that context might be clouded or inadmissible. What help can you give me on that issue?

Ms Jackson—The advice that we had from the Office of International Law was that if we used surveillance devices on what is basically foreign soil—that is, a foreign flagged vessel—outside Australian territorial sea for general offences, outside the contiguous zone for the fiscal/customs/quarantine offences and outside the fishing zone for fisheries offences, we would be in breach of international law if we did not have the consent of the flag state.

Senator SCULLION—So FOC vessels are exempt—the flag of convenience vessels that do not actually profess to belong to anywhere.

Ms Jackson—Yes.

Senator SCULLION—The issue of the consistency of the legislation has been a theme of discussion. There are privacy issues and the issue of ensuring that the information does not fall into the wrong hands by destroying it when it is no longer needed. I would have thought that it would be consistent whether it is a search warrant, an SD warrant or telecommunications intercept warrant. Clearly we have differences—whether you report it to the minister or parliament, although that has apparently been clarified, and there are differences between the 48 hours and the 24 hours. It is not clearly articulated that there is no civil remedy in terms of one act and not the other. Why is it that we have that sort of approach in view of the fact that those issues are pretty much, I would have thought, outside the content of the issues? If that is simply a process about privacy, efficacy and transparency, why would we have any differences there at all?

Ms Jackson—That is a historical issue. Our bill is modelled largely on the joint working group model rather than specifically on the telephone intercept legislation. That was a choice government made.

Senator SCULLION—Would it be reasonable to say that the differences that are identified are those differences that are articulated in the working group's recommendations?

Mr Smith—There is also the constitutional aspect. As Maggie said, the T(I) Act is the complete regulator of all TI matters. The civil remedy must exist in that act otherwise it will exist nowhere. As was raised this morning, if somebody unlawfully puts a listening device on your property, what sort of remedy do you have? You could sue them civilly for trespass and obtain damages and have that transcript destroyed. That would be the existing civil remedy there. If we did not have civil remedy provisions in the T(I) Act they would not exist anywhere.

Senator LUDWIG—What if there was not a trespass offence—if they were next door with a sophisticated listening device and got the wrong house?

Mr Smith—The warrantless provision, referring to clause 37 of the bill which relates to the use of an optical surveillance device without a warrant, only relates to optical surveillance devices where there is no trespass. We would have to think about this but if you were, to use an example used earlier, distant and using one of those remote mikes to pick up conversations on private property that use would not be covered by the optical surveillance device power in clause 37 so arguably you would need a warrant, I think. I can check that.

Ms Jackson—Yes.

Senator LUDWIG—If you were sitting next door using an infra-red camera?

Mr Smith—You have to consider what happens with infra-red cameras because they are not specifically dealt with in this provision.

Senator LUDWIG—Are you saying that they are not an optical surveillance device?

Mr Smith—It is arguable whether they are or are not. The Victorian Privacy Commissioner gave the example of the Kyllo case in the United States where the infra-red looked straight through the walls of a house. It is very arguable whether that would be an optical surveillance device. We would have to consider that.

CHAIR—What else would you call it?

Senator LUDWIG—By definition.

Mr Smith—An infrared optical surveillance device. We would have to—

CHAIR—We asked whether or not this was technology neutral, because that was raised with us, and were told it was essentially technology neutral. If an infrared observing process is not an optical surveillance device, what is it?

Mr Smith—We have defined an optical surveillance device as any device capable of being used to visually record or observe an activity. In that sense, an infrared device does that. But it is certainly not within the spirit of this bill and we would have to consider that.

Senator LUDWIG—Infrared, if you look at it from a science point of view, is part of the spectrum of light.

CHAIR—How is it not within the spirit of the bill?

Mr Smith—It was not considered part of the process—that is, we were never faced with law enforcement agencies using infrared. We are not aware that they do it. They may do, but it was not considered part of this process.

Senator LUDWIG—They do in the States—there has been a case about it.

Mr Smith—Yes.

Senator LUDWIG—So, did you take that into consideration?

Mr Smith—Not as part of this bill. The police never indicated that they used infrared technologies like that in the Kyllo case.

CHAIR—So is that something you would be bringing forward in regulations?

Mr Smith—Alternatively, you could clarify in the EM the definition of 'optical surveillance device' to indicate that it meant ordinary optical surveillance technologies and not such things as infrared.

CHAIR—I do not think there is any such thing as an ordinary technology, Mr Smith!

Senator SCULLION—Would that be defined as those not requiring a warrant?

Mr Smith—An optical surveillance device under this bill can be warranted or warrantless, depending on the circumstances.

CHAIR—Senator Scullion is asking if this device would fall into the category of—

Senator SCULLION—warrantless or warranted.

Mr Smith—We would hope that infrared uses would involve a warrant.

CHAIR—'We would hope' is not very reassuring to the committee.

Mr Smith—No, that is right; it is not.

Senator SCULLION—I have asked the Australian Federal Police to provide me with a list of those processes that they believe would not require a warrant. I know that privacy advocates would certainly be looking for something more prescriptive. I know we have tried to keep away from technology, but, as you say, perhaps in the EM or in a regulatory sense we could continue to update without changing the act.

Senator LUDWIG—I would not mind you clarifying that the application of remote listening devices that do not include the trespass of land requires a warrant.

Mr Smith—Clause 37 is about the warrantless power—the use of optical surveillance devices without warrant where it does not involve trespass or interference with private property. It specifically refers to optical surveillance devices, not listening devices. So a remote mike, which would pick up conversations over some distance, would be a listening device rather than an optical surveillance device and hence would not be covered by this power.

Senator LUDWIG—In short, you are saying that a remote listening device that does not involve trespass would require a warrant.

Ms Jackson—Yes.

Mr Smith—Yes.

Senator LUDWIG—But it may still fall within an emergency warrant?

Ms Jackson—Yes.

Mr Smith—A listening device can be used under an emergency authorisation, yes.

Senator LUDWIG—Thank you.

CHAIR—Can you tell me if I am reading section 14(7)(b) correctly. I read it as saying that where, as it says under section 14(3), the application for the surveillance device warrant pertains to a situation where 'a recovery order is in force' or the LEO 'suspects that the use of a surveillance device may assist in the location and safe recovery of the child to whom the recovery order relates', the affidavit does not have to be provided to the eligible judge or nominated AAT member for 72 hours. Is that right?

Mr Smith—That is what it says, yes.

CHAIR—Why is that a different time frame from the 48 hours?

Mr Smith—I imagine that would have come from the model bill.

CHAIR—I was keen to get Mr Duggan involved, you see. If someone else can tell me, I am still keen to have an answer as to why it is different. If you cannot answer it today—

Ms Jackson—I think they are different in the model. I think that one is 72 hours in the model and the other one is two business days.

CHAIR—We seem to have some inherent differences—I will not call them inconsistencies until we get some clarification—on some of these time frames. We had some operational advice, which I thought was helpful, from the AFP in relation to some of these matters. There seems to me to be no obvious explanation for that, so perhaps, Ms Jackson, you might take those differences as a question on notice.

Ms Jackson—That is at clause 7(5) in the model bill, and it is 72 hours there.

CHAIR—If there is some advice you can give the committee as to why we should support that difference, that would be helpful.

Mr Smith—The difference from the TI act?

Ms Jackson—No, the difference being two business days.

CHAIR—The difference within this bill is between two business days and 72 hours. Not even the terminology is consistent.

Mr Smith—The emergency authorisation process is different from the provision of an affidavit after a telephone application.

CHAIR—But you would think it would be in the same units, at least.

Senator LUDWIG—Clause 17 provides that the LEAs are not required to report back to the judge who issued the warrant but instead to the minister. Why would you not go back to the judicial officer?

Ms Jackson—That is something that does not exist in any Commonwealth legislation. The idea of reporting back to the judge who issued the warrant comes from Victorian legislation.

Senator LUDWIG—It was raised in the privacy commission submission.

Ms Jackson—The advice that we had from Victoria was that their reports are in writing and are filed with the court documents. This did not really seem like a terribly successful oversight regime to us, so we discussed it with the AAT. The AAT said they did not wish to have these records that required secure storage and so on. Reporting to the minister and the parliament seemed a much more satisfactory regime and it was more consistent with similar regimes in Commonwealth legislation.

Senator LUDWIG—In relation to the destruction, why wouldn't you have an independent oversight of the destruction of the records?

Ms Jackson—We require the agency to keep a record of the destruction and for that to be available to the Ombudsman. I do not know how feasible it would be to have somebody physically present when these records are destroyed. I would imagine that there will be a very significant number of these that are destroyed on a more or less continuous basis. I do not think that you could batch them up and then destroy them every three months or so. That really would not be consistent with the philosophy of the legislation of destroying them when you decide that they are no longer relevant.

Senator LUDWIG—Perhaps you could find out from the AFP and the ACC how they go about the destruction of their records and advise the committee whether they batch them up or destroy them continuously. The Office of the Victorian Privacy Commission also raised the issue that the recording of conversations by or on behalf of police should only occur with the appropriate judicial oversight. Is there a reason that you do not include a warrant for that?

Ms Jackson—That is already in the existing Commonwealth legislation to enable undercover operatives to wear a wire—the stinger-type stuff. It was taken directly from 12G of the AFP act.

Mr Smith—It is also considered important for the safety of the officer that they always have access to a wire if they go under cover, for example.

CHAIR—Finally, back on the question of emergency authorisations, they are basically made without any sworn evidence, aren't they? A police officer just applies to a more senior officer to get an emergency authorisation for the surveillance device.

Ms Jackson—Yes. Then under 33(2)(b) you need the affidavit when you take it to court.

CHAIR—But that is after the surveillance has already been implemented.

Ms Jackson—True.

CHAIR—I imagine that we regard these as pretty serious powers—powers not to be used lightly by law enforcement agencies. But, as I understand it, even with a telephone application for a search warrant you still have to fax an affidavit to the authority before you are granted a telephone search warrant.

Mr Smith—You mean a remote application by telephone under the TI act?

CHAIR—Yes.

Mr Smith—I think, having had a look at this before, that you can supply the affidavit one day later. Section 51 of the TI act states:

(1) A person … who makes a telephone application on an agency's behalf shall comply with this section within one day after the day on which a warrant is issued …

(2) The applicant shall cause each person … to swear an affidavit setting out the information so given by the person.

I think that requires the affidavit to flow one day after the telephone application.

CHAIR—That would be ex post facto, obviously.

Mr Smith—Yes.

Senator SCULLION—I turn to evidence that is taken but is not subsequently authorised. The Australian Federal Police were asked: 'Why don't you think this evidence should be destroyed? Obviously, it is not to be used for evidence.' They said, 'We need to keep it hanging around just in case there are proceedings against our people.' That seems quite reasonable. If that evidence is not admissible—and we now know that it has not been destroyed—there is no provision to say a police officer cannot use it; for example, in further record of interviews. It is not evidence; it is just a record of interview. We can use that to glean other evidence, which is then lawful evidence that is admissible. I do not know a great

deal about this stuff. I might have the wrong end of the stick here. But it just seems that there is a process whereby if it is not subsequently authorised, it is not destroyed. So it can still be used by a police officer or some agency. That officer or agency can then translate it, if you like, into admissible evidence by bringing it into play in a record of interview or some other process to validate it, or they can have someone validate it in some other forum. That seems that it is not really a check and balance.

Mr Smith—The offence provisions of the bill which apply to protected information make it an offence to further communicate—further use—protected information. Protected information is defined under clause 44 as:

(a) any information obtained from the use of a surveillance device …

(b) any information relating to:

(i) an application for … a warrant …

(c) any information that is likely to enable the identification of a person, object or premises …

So it is a very broad definition of information that results from or relates to a warrant. It does not specify the medium, so just because you have then entered into an interview of record—which you could do with regard to lawful information but not unlawful information—the offence provisions still apply. That information is still unlawful. You still cannot communicate or disclose it except with regard to the exceptions.

Senator SCULLION—But you can understand, Mr Smith, how vague that must appear to someone like me. We know that we have been having a good look at this bloke. He has a white caravan and a blue car in his backyard, and we know that they are full of something you are not supposed to have. He does not have to talk about anything. You might just have to say, 'What's in your backyard, mate?' It is pretty long-ended. Within the broad structure, I understand the intent of that. I am not so sure how it would look from the perspective of somebody who is looking at it from the outside. They will expect our committee to make sure that there is some transparency in this process. The fact is that the police still have that information. They have not been asked to destroy it. The judge has said, 'This information is not admissible.' The Australian Federal Police said that they may in some circumstances wish to use the evidence that was taken as evidence to prosecute. Apart from that one issue, are there any other real issues that mean you would want the police to hang on to the information?

Mr Smith—There are three basic issues. One is the possible prosecution of the police themselves, the second is the ombudsman investigation to have a look at what has been done, and the third is the national security issue of ASIO and intelligence agencies.

Ms Jackson—And privacy.

Senator SCULLION—We would assume that the Australian Federal Police would hang on to it for the purposes of territory or state legislation, which is the only legislation under which they could prosecute somebody—let us say for taking it incorrectly. I suppose that is a slightly different circumstance.

Mr Smith—Or internal police proceedings.

Ms Jackson—But if they use it incorrectly it is a breach of clause 45. If you want to follow it through, 44(d)(ii) includes information that is obtained under an emergency authorisation that is not subsequently approved. Clause 45(6) says that you cannot use it for a purpose that appears in paragraphs (5)(a), (b) and (c)—and (5)(a) is the investigation of the relevant offence. That then links into the offence provision to which Nick referred, that says that where the person uses protected information they are guilty of an offence.

Senator SCULLION—When I first read that I got the view that, if you get some information lawfully—because you have gone through the process—and it is then deemed to be unauthorised, in fact that information probably comes under less review than information that is taken the other way. There does not seem to be any limitation. Does that information that is now not authorised still come under the purview of the ombudsman?

Ms Jackson—Yes.

Senator SCULLION—So it will come under exactly the same circumstance as the other material?

Ms Jackson—Yes.

Senator SCULLION—So you are telling me that, if it is no longer required, if there is a meeting they will simply say, 'Okay, do you have any policemen you wish to prosecute on this?' They will say no and you will say, 'Right, it's obvious that this has reached the stage where it now needs to be destroyed.'

Ms Jackson—That is theoretical.

Senator SCULLION—So within that process I can have some confidence that this information is not going to hang around forever, in any event.

Senator LUDWIG—Except that which is in the officer's mind.

Senator SCULLION—Of course. Thank you, Chair.

Senator LUDWIG—Is subsection 12G(6) of the Australian Federal Police Act reflected here as well? It was raised in a submission by an assistant lecturer at Monash University, Patrick Emerton. He referred to paragraph 18(1)(a), which permits:

... a surveillance device warrant to be issued with respect to premises. The issue of such a warrant clearly poses a threat to the privacy of those who use the premises in question, but who are not suspects in an investigation. Given this threat to privacy, the Bill does not seem to impose sufficient restrictions on the issuing of a warrant with respect to premises (for example—

that which is—

under subsection 12G (6) the *Australian Federal Police Act 1979*).

I was just trying to work out whether that is right. If it is right, why wouldn't you? I am happy for you to take that on notice.

Mr Smith—I can answer now, I think. The provision, as I understand it, says to consider the privacy implications with regard to premises. There are other provisions which consider the privacy implications with regard to this or that. When you seek a warrant, the AAT member or the judge says that you have to consider any privacy implications. We do it generally rather than with regard to premises, an object or a person.

Senator LUDWIG—The validity of the warrant is 90 days, whereas under the TI legislation it is 60 days. In the sense that this warrant hangs around for a very long time, especially if it is the type that you have described, what are the reasons for the additional 30 days?

Ms Jackson—That is something that was very actively debated in the joint working group. Some jurisdictions have much shorter periods of one month, and other jurisdictions have six months. Three months was the compromise that was accepted by everybody.

Mr Smith—There are also basic operational reasons for the difference between SD and TI. With TI you switch it on and you switch it off with a phone call or a warrant faxed to the phone company. With SD, of course, you might be talking about a device which is located on someone else's premises, and you have to go and get it back, for example, which might take time. So it is quite a different physical process.

Senator LUDWIG—Do you have to retrieve it?

Mr Smith—Install it and then retrieve it later on, which is much harder than TI.

Senator LUDWIG—And not turn it off. Thank you.

CHAIR—Ms Jackson, there are a couple of questions you have taken on notice, and the secretariat will follow up those questions with you. I thank both you and Mr Smith very much for your assistance today. I want to thank all of the witnesses who have given evidence to the committee today, and I particularly thank the secretariat of the Joint Statutory Committee on the Australian Crime Commission for their assistance with preparation and support for senators for this hearing.

Committee adjourned at 1.04 p.m.