COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE

Reference: Telecommunications (Interception) Amendment Bill 2006

WEDNESDAY, 15 MARCH 2006

S Y D N E Y

BY AUTHORITY OF THE SENATE

INTERNET

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

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

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

SENATE

LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE

Wednesday, 15 March 2006

Members: Senator Payne *(Chair)*, Senator Crossin *(Deputy Chair)*, Senators Bartlett, Kirk, Mason and Scullion

Participating members: Senators Abetz, Allison, Barnett, Bartlett, Mark Bishop, Brandis, Bob Brown, George Campbell, Carr, Chapman, Colbeck, Conroy, Eggleston, Evans, Faulkner, Ferguson, Ferris, Fielding, Fierravanti-Wells, Heffernan, Hogg, Humphries, Hurley, Johnston, Joyce, Lightfoot, Ludwig, Lundy, Ian Macdonald, McGauran, McLucas, Milne, Murray, Nettle, Parry, Patterson, Ray, Sherry, Siewert, Stephens, Stott Despoja, Trood and Watson

Senator Bartlett for matters relating to the Immigration and Multicultural Affairs portfolio

Senators in attendance: Senators Kirk, Ludwig, Payne, Stott Despoja

Terms of reference for the inquiry:

Telecommunications (Interception) Amendment Bill 2006.

WITNESSES

Committee met at 9.39 am

CHAIR (Senator Payne)—Good morning, ladies and gentlemen. This is the hearing for the Senate Legal and Constitutional Legislation Committee's inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006. The inquiry was referred to the committee by the Senate on 1 March 2006 for report by 27 March 2006. The bill amends the Telecommunications Act 1979 to implement certain recommendations of the *Report of the review of the regulation of access to communications*, known as the Blunn report.

Specifically, the bill amends the act to establish a regime to govern access to stored communications, to enable the interception of communications of a person known to communicate with a person of interest, to enable the interception of communications from an identified communications device, to remove the distinction between class 1 and class 2 offences for which telecommunication interception powers are currently available and, finally, to remove the Telecommunications Interception Remote Authority Connection function currently exercised by the Australian Federal Police and transfer the associated warrant register function to the Attorney-General's Department.

The committee has received 17 submissions for this inquiry and is processing submissions. Those submissions which have been authorised for publication are available on the committee's website. 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 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.

[9.41 am]

JAYAWARDENA, Ms Pradeepa, Policy Lawyer, Law Council of Australia

NORTH, Mr John, President, Law Council of Australia

Evidence was taken via teleconference—

CHAIR—Welcome, Mr John North, President, and Ms Pradeepa Jayawardena, Legal Policy Officer, representing the Law Council of Australia who are both appearing via teleconference. The Law Council has lodged a submission, which we have numbered 17. Do you need to make any amendments or alterations to that submission?

Mr North—I have three. On page 6 at item 21, it should read 'potentially be targeted.' So the words 'by the AFP and ASIO' should be deleted. On page 8 at item 30, the second line should end with 'expressed in the Blunn report.' So the words 'including in relation to fishing expeditions' should be deleted. In item 32 the first sentence should read 'A safeguard that is incorporated in clauses 3 and 9 of the bill provide that the Attorney-General, judge or nominated AAT member ...'. I think that is it. We have had to do this in haste, as you have had to convene in haste, so we apologise for that.

CHAIR—We thank you very much for the submission; we are very grateful for that. Senators may not have had a chance to read the whole thing but we certainly have the gist of the council's views. I invite you to make an opening statement and then we will go to questions.

Mr North—The Law Council of Australia is pleased to attend this public hearing in relation to the Telecommunications (Interception) Amendment Bill 2006. The Law Council is the peak national representative body of the Australian legal profession. It was established in 1933 and represents federally approximately 50,000 Australian lawyers.

Due to the limited time provided to review the bill, the Law Council's submission has raised some serious issues and concerns with respect to the controversial measures contained in schedule 2 of the bill, namely B-party interception. The Law Council strongly and unequivocally opposes measures in schedule 2 of the bill. The Law Council urges the government to abandon proposals to allow telecommunications surveillance of innocent people. Persons not suspected of crime should not be subjected by the state to surveillance. This proposal abrogates fundamental freedoms and human rights of people not suspected of any crime or wrongdoing. In fact, we believe this is the first time ever in Australia's history that law enforcement agencies will be given power to intercept telecommunications of people who are not suspects, who are innocent people. We ask the government to answer this question for the public: is the proposed measure necessary and are these proposed laws proportionate to the threat that we face?

In schedule 2 of the bill, the right of an innocent to a life free of unlawful interference with his or her privacy, family and home is eroded in an attempt to gather evidence in relation to alleged ordinary crimes. We point out at this stage that this bill proposes to relate to crimes that carry prison terms of seven years or more. That covers a great raft of criminal offences in relation to which we will be allowing government agencies to listen in to the calls of innocent people. We believe that the proposed measure appears to be disproportionate to the perceived

threat to the Australian people in allowing this interception of the telecommunications of innocent people in relation to people who are committing ordinary crimes. The Law Council submits that schedule 2 of the bill breaches the right to privacy, which is a fundamental human right guaranteed under the International Covenant on Civil and Political Rights and other international instruments and is entrenched in Australian legislation, including the Privacy Act 1988 and legislation in the states and territories. In particular we have set out that it is a breach, in our view, of article 17 of the ICCPR.

The proposed law fails to have proper limits, controls and safeguards. All Australians can potentially be targeted. Children, family members, colleagues, lawyers, doctors and priests going about their work may be targeted. There are no exemptions in respect of confidential communications, and it is even unclear whether legal professional privilege is abrogated. You will note that in our submission we discuss this in more detail. This is bad law.

While the Law Council opposes the whole of schedule 2 even being enacted, if these laws are going to be brought in by the government, we strongly urge it to ensure that they are accompanied by proper legal safeguards and protections, which include the following. There should be guidelines clarifying the scope of who can be monitored as a B-party. For instance, factors including the frequency of contact should be expressly stated in the legislation. If the intention is that schedule 2 should apply as a last resort, the interception warrant should only be available for investigations of very serious offences—for instance, class 1 offences such as murder and terrorist offences—and not be allowed to cover the majority number of criminal offences.

The Law Council has serious concerns about extending the power of the Attorney-General to issue these telecommunications interception warrants in respect of innocent third parties. We believe that there needs to be a real judicial function here, and we set that out in our paper. There is, you will note from the old bill, which was enacted in 1979, provision for rolling over interception warrants. When you think about rolling over interception warrants in relation to innocent people, the mind boggles. We believe that there should not be any rollover unless a judicial officer can be shown that some very useful or crucial information from an earlier warrant was gained.

As I have said, we believe that this should be subject to independent review at least every two to three years after its commencement. We also believe that there should be a sunset clause incorporated in the act, consistent with other legislation which erodes our fundamental human rights. We believe that the measures should contain express exemption categories and these should include communications with lawyers and doctors and perhaps should look at the clergy as well and at the position of children. The proposed measures should expressly provide that schedule 2 does not abrogate legal professional privilege.

In relation to reporting we say that each year the government should be required to report specific details, including the number of applications by agencies for interception, the number of warrants issued by the Attorney-General, the grounds upon which they were issued and the safeguards in place to prevent abuse. We should be able to look at those statistics in a meaningful way so that they are broken down between those that are issued in the normal course for people who are suspected of being involved in crimes and those that relate to innocent people.

In conclusion, we reiterate that we think this is very bad law. We cannot see the justification for it. If you consider what has happened when we allow the government in other areas to deport people under the extradition laws or to restrict freedoms, as has happened in the antiterrorist field, this is just one more law that is going to make this a very, very unpleasant country to live in. We do not understand how this is going to help us in the fight against terrorism and other serious crimes, but we do understand that if this law passes into the statute books then every single Australian will from now on not know that their private calls or telecommunications are liable to be listened to by a government agency. Nothing more fundamental or important has come across our desks in a long time, apart from our discussions on the previous antiterrorism legislation. Thank you very much for listening.

CHAIR—Ms Jayawardena, do you want to add anything at this stage?

Ms Jayawardena—No.

CHAIR—I am interested in the Law Council's proposition particularly in relation to the issuing of warrants under schedule 2 for what is called B-party interception and your concern about that role being given to the Attorney-General rather than to a judicial officer. For a warrant of that nature, are you aware of any precedents where the authority has been given to an office holder such as the Attorney-General rather than to a judicial officer?

Mr North—In our submission to you we have talked about the fact that a parallel can be drawn with the detention of unlawful noncitizens pursuant to the Migration Act being done as an executive function rather than having a proper judicial oversight. We all know what has happened as a result of that. You have the circumstances of Cornelia Rau and Vivian Alvarez, and it leads to—

Senator LUDWIG—I do not want to interrupt you, but the concern I have in going down that track is that I am not too sure whether I agree with the parallel. I see that in your submission. However, if you look at the discretion under 417 and elsewhere in the Migration Act you see that it is an extraordinary power. It is one that I am quite happy to say that I am trying to circumscribe and have tried on a number of occasions to do so because it is unappealable and a total discretion. It rests with the minister, who then does not have to provide any grounds or reasons to substantiate why the decision was made. It is one of those powers that were supposed to be an end of the line catch-all where there was an unusual circumstance. Since that time it has blown out into a discretion that is at large for the minister to exercise.

Mr North—I think you make a good point there, Senator. I will not press down that path, but I was asked by the chair if we knew of anything else. What we are really saying is that it seems to be fundamentally wrong to give to the executive branch of the government such a wide-reaching power to seek the issue of warrants to listen to innocent people. We have nothing against the Attorney-General personally, but we say this must be judicially oversighted because it is such a far-reaching thing.

Senator LUDWIG—I see your point.

Mr North—So, to answer your question, I do not know of any other example.

CHAIR—You cite in your submission in paragraph 29 some of the observations of Mr Blunn in his report in relation to B-party intercepts. In subparagraph (d) of those points made by Mr Blunn, some of the safeguards which he suggests might be in place to deal with the idea of B-party intercepts are raised. Some of those are quite attractive as far as I am concerned. This is just the beginning of this process today, but they are obviously cited positively by the Law Council. You would think that they are useful safeguards to have in place?

Mr North—Yes. If your government is going ahead with this act in the form that it is then these are absolutely essential. We have also set out some of the other things, which I went through, that we would like to see put in place. We do agree that they are absolutely essential and that they are appropriate, but we still do not resile from the fundamental proposition that our government should not be listening to innocent people.

CHAIR—I understand that. It is a perfectly reasonable proposition to start with.

Senator KIRK—Thank you, Mr North, for your submission and for your comments here today. I would also like to follow up on this power of the Attorney-General to issue the interception warrants with respect to innocent third parties. I hear what you are saying about the problems that arise with the Attorney-General having that power. You have emphasised in your submission that there ought to be judicial oversight of these matters. Are you suggesting to us that the Attorney-General should be removed from the list of persons who can issue warrants or just that there ought to be some kind of judicial oversight of his or her decisions?

Mr North—It is a good question. I should clarify this: I think the existing act, under section 9, allows the Attorney-General, upon the request of the Director-General of Security, to issue the warrant. That is already in the existing act, so I hope that answers the question. What we are saying is that that act relates to where police or other agencies suspect someone of being involved in a criminal act. We have lived with that act since 1979 and we can continue to live with that act. What we are saying is that we do not believe the executive government, in the guise of the Attorney-General, should be allowed to do this in relation to innocent people. I hope that has clarified our point. We believe that it should be judicially oversighted because it is such a huge invasion into every single Australian's right to privacy. So it is already there in the act, and I apologise: I was trying to think wider than the act itself when I was listening to the question.

Senator KIRK—So with respect to this legislation you would like to see the Attorney-General's role removed entirely?

Mr North—No.

Senator KIRK—Or just judicially oversighted?

Mr North—The act will still have its old operative provisions in which, if authorities suspect someone of something, they can apply in the normal course, and should apply in the normal course, to try to get a warrant. But what we do say is that, for innocent people being listened to, that should not be a function of the executive government. It would need the act as it stands now, as it is before you, to be changed in that regard.

Senator KIRK—What about with respect to the power of other individuals—for example, judges, which would seem okay, but also members of the AAT and other officers—to issue warrants?

Mr North—We would ask the government, if they are going to bring in this legislation, to repose that power in such people, in those judicial officers—

Senator KIRK—Only?

Mr North—so that they could then be absolutely assured that this third-party listening is going to have some efficacy—that there is some reason for it. They have tried to set out the reasons there in the new bill, and I will not go into that, but we are saying that this should be judicially oversighted from the very beginning, from when the warrant is being sought.

Senator LUDWIG—For those issues that are detailed in the Blunn report in respect of B-party intercepts, it sets out a number of points—that is:

> ... a requirement that any agency requesting such a warrant must establish to the satisfaction of the issuing authority evidence to support their belief that the information likely to be obtained from the intercept is material to the investigation.

There are about four points. Have you had an opportunity to look at those and say whether you similarly adopt them? If you have not then I am happy for you to take that on notice. I understand your immediate objection to the legislation.

Mr North—I will say in answer—and we might follow this up, but I have not individually put my mind to that—that we would support anything that employs more safeguards, if the legislation is going ahead. But I have and we have a fundamental difficulty with seeing what is behind this. If you look at what they are trying to achieve—and Blunn seems to gloss over this; he seems to say that he can see that there might be some purpose in having these B-party intercepts—and if you accept that a B-party intercept is against an innocent person, in other words, a person whom the authorities do not suspect in any way of being involved in any crime, what utility is there going to be in allowing their communications to be intercepted and listened to? Someone who is going to commit a crime is hardly going to suddenly join them into the conspiracy. If the authorities thought that the person was going to be joined into the conspiracy then the existing act is perfect to get a warrant.

So the threshold question must be asked: why are innocent people being targeted under this legislation? There seems to be a fundamental gap in the reasoning in Blunn and everywhere else as to why they want it. The Attorney-General seems to say that criminals are adept at changing phones and doing other things, but they are also quite often, in most of the cases I run now—big drug cases and everything else—caught by their use of mobile phones, with properly instituted warrants under the existing law. What is the purpose? Maybe you are at the beginning of your investigations, but it is something we would ask you to keep in mind when you talk to the authorities: how is this huge invasion of privacy going to be justified?

Senator LUDWIG—That is a challenge for the Attorney-General. Have you had an opportunity—and you may not have, given the limited time—to look at the submissions from EFA, Electronic Frontiers Australia? I ask you—and you might want to take this on notice—to go to page 28 of their submission. At point 131, they say:

If, at some future time, we were to become persuaded that such interceptions should be permitted in some clearly specified and limited circumstances, we would consider that, at the very least, the following safeguards and controls would need to be implemented ...

I do understand your earlier evidence that, although you oppose it, any improvement would be seen as a positive. But, if you could have a look at those issues (a) to (e) that they have said should also be included, the question is whether they have any utility, whether they can be effective and whether they in fact add to ensuring that there are safeguards and controls in respect of that.

Mr North—We would like to have a look at that because—not knowing what is there—they may well add to improving the situation if the law goes through.

Senator LUDWIG—The other issue that has been raised is in, I think, Mr Kerr's submission, which went to use and derivative use. I think Electronic Frontiers may have mentioned it as well. With B-party intercepts, as you would be aware, it would also be in respect of parties C, D, E and F, which might also be recorded.

Mr North—That is right. One of the real problems with this is that, once you start going down this path, if you have unscrupulous operators in any of the authorities and so forth, what they learn—which may have nothing to do with the crime but is something else about some other proposed business deal crime or someone's personal lifestyle—can lead us into a very ugly area. You have to understand that there will be people who will be transcribing and listening to the tapes, and we will be relying on their good judgment not to interfere in our citizens' lives. It is a dreadful prospect and you can try to put all sorts of safeguards in there, but you still have to go back to the fundamental question: why are we going to do this?

Senator LUDWIG—I did not want to dissuade you from that course. It is just a question of whether you want to also have a look at use and derivate use immunity—whether it had any utility in that area.

Mr North—We will have a look at that. Use and derivative use is something we have discussed. It also falls into the other part that I have not mentioned much: what effect is this going to have on legal professional privilege; what effect is this going to have on self-incrimination? Something else will come out of one of these phone calls. You have to consider a criminal lawyer such as me. If I am subject to a phone tap, all sorts of people might be ringing me with nothing to do with what the phone tap is about, but they might sometimes say pretty stupid things on the phone to me. Last year a fellow confessed over the phone three times to murder but he was innocent and I got him off despite his protestations.

Senator LUDWIG—I probably do not need to know that.

Mr North—It does not matter; it is finished. But he was not guilty; he was doing it for other reasons.

Senator LUDWIG—You do not have to explain. I always say: 'When you've got a shovel, stop digging.'

Mr North—That is right. But real, proper controls are necessary to regulate use and derivative use. If some of these are set out in the reports we have not seen, we will try to get back to you in the short time we have.

Senator LUDWIG—Yes. The timing is that of the government, if we want to blame someone.

Mr North—We have continually requested time for such important matters—and it is not the fault of the committee, because you have a very short time to report—and it is something that we hope the committee will take back to the government when we talk about these things in the future.

Senator LUDWIG—It is a matter I will raise. The other area is 'named person warrants'. I am trying to get a sense of the difference between B-party and named person warrants. Named person warrants can obviously name a person and seek a telecommunications interception warrant in respect of that person. You say that that is different from a B-party.

Mr North—Yes, because the named person is somebody who the authorities—I think, the director-general of security—believe is either engaged in or reasonably suspected of being engaged in some sort of criminal act. We have no real problem with that—that is the way the act operates—but the B-parties can cover, and are contemplated to cover, innocent people.

Senator LUDWIG—Thank you. That is very helpful.

CHAIR—Mr North, one of the issues that is an aspect of this bill is that the proposals will permit applications for warrants to be made by agencies that are responsible for administering a law which imposes a pecuniary penalty or administering the law relating to the protection of public revenues. That might include the Customs service, the tax office, ASIC and so on. The Ombudsman, in his submission, raises the expansion of agencies that will be able to make such applications and notes in his section that there will not be a government approved list of agencies which might apply, as there is currently under section 34 of the act. Does the Law Council have a view on that matter; on that expansion and how to manage that process appropriately?

Mr North—Yes. We believe it should not just be a carte blanche to any government agency. At the moment, I think the way to attack it is not to have a list of government agencies that can or cannot be allowed to apply. On our submission, they should be allowed to apply only if it relates to a class 1 offence, such as murder and/or terrorism. We cannot have every single government agency in the country listening to innocent citizens in the hope they will catch them on some tax fraud or something else. It is absurd, and that is the problem with the changes to the bill which purport to allow this for any crime that carries seven years or more. That is a fundamental point, and one we really hope that you will take on board. How dare our government listen to people all around this country in the hope that they will pick them up for some fiddly little matter. Any criminal lawyer will tell you nearly every charge in the Crimes Act now carries, because of the endless law and order debates we have in each state and territory every year, seven years or more—any indictable crime.

CHAIR—My learned colleague Senator Ludwig points out that the nomenclature is changing to 'serious offence' from 'class 1 offence' and other offences anyhow, so in fact the distinction is blurring right through the legislative process.

Mr North—That is a very good point, and you would see no end to this. If this bill goes through in its present state, you will have all of those government agencies—all of them—having a look to see whether they can pick up people for crimes that are not threatening the

security of the country, such as terrorism would, or for crimes that are not normally serious, such as murder would be, for which these intrusions into privacy may be justified in some circumstances.

CHAIR—The other point the Ombudsman makes is that, if the bill is passed, the impact that it will have on the role of the Ombudsman and his resources is a significant one. The committee has long been grateful to the Ombudsman's department for its submissions to the work that we do, whether it is counter-terrorism more broadly or this sort of thing. Does the Law Council have any comment to make in relation to the role of the Ombudsman, and particularly the telecommunications interception monitoring process and inspection process?

Mr North—As we said in our submission, we would hope there is regular and open reporting, and if this is to be oversighted by the Ombudsman then so be it. That would be a good starting point. But the material that is reported at the moment under the existing act is really impenetrable, and you do not really know what is happening. If you are going to move down the path of having innocent people phone-tapped and listened to, you must put in a regime whereby there is clear, adequate, good reporting and proper oversight. I think the Ombudsman's office has shown in other areas that it is willing to take on these hard matters, but that would of course then be a matter of resources for the government to look at.

CHAIR—Indeed, and a matter for the committee to consider as well. As there are no more questions, Mr North and Ms Jayawardena, thank you very much for your time this morning. We do appreciate your agreeing to appear by teleconference. I know we were trying to organise for you to attend the committee, Mr North, but it has been very helpful for you to appear this morning at the beginning of our proceedings.

Mr North—Thank you very much. I will say one thing about oversight of all these things that need to be taken into account, whether it is by the Ombudsmen or judicial oversight or anything else: the insidious thing about having innocent people being listened to in this way is that they do not know that they are being listened to, so they have nowhere they can go and complain and say, 'This should not have happened.' So, when you are thinking about whether these laws are necessary and proportionate, we would ask you to take that into account.

I am sorry I was not there face to face. I had it in my diary for four o'clock this afternoon in Canberra, not knowing that you were sitting in Sydney, and then I had to be here anyway.

CHAIR—No problem. Thank you, Mr North.

Mr North—Until next time, thank you very much.

[10.16 am]

GRAHAM, Ms Irene Joy, Executive Director, Electronic Frontiers Australia Inc.

CHAIR—Welcome. Electronic Frontiers Australia has lodged with the committee a submission, which we have numbered 3. Do you need to make any amendments or alterations to that?

Ms Graham—No, we do not, thank you.

CHAIR—Then, Ms Graham, I will ask you to make an opening statement and then we will go to questions.

Ms Graham—As we have submitted a very extensive submission, I will not take a lot of time with an opening statement. I would just like to reiterate that, generally, we support the stored communications provisions but we do have some problems with some of the definitions, particularly in relation to whether a copy of a communication is also a communication for the purposes of the act. We also note that some of the safeguards and accountability measures for stored communications are significantly less than for interception warrants, and we do not believe they are adequate at all.

We also have some concerns about the interrelationship between the interception act and the Telecommunications Act, insofar as, for example, section 280 of the Telecommunications Act is not being amended. We believe there is a lack of clarity as a result as to whether civil penalty enforcement agencies will be able to use notices-to-produce at carriers' premises or whether in fact they need a stored communications warrant, as would seem to be indicated by the Telecommunications Act.

CHAIR—I am sorry, Ms Graham, could you say that again?

Ms Graham—Section 280 of the Telecommunications Act, not the interception act, provides circumstances in which carriers can disclose copies of communications to law enforcement agencies. In our view, that makes quite clear that an enforcement agency—be it a criminal law enforcement agency or a civil law penalty agency—cannot receive copies of communications from carriers unless they have 'a warrant'. However, there are a number of agencies, such as ASIC and the ACCC, who seem to be under the impression that they can submit a compulsory notice-to-produce under their own legislation and expect carriers to provide copies of communications.

We believe that the Telecommunications Act overrides that and therefore, once the interception bill is passed, it will then override the Telecommunications Act and, as a result, civil penalty agencies and criminal penalty agencies will need to provide a warrant. There are no notice-to-produce provisions. But the explanatory memorandum states that civil penalty agencies will be able to issue a notice-to-produce to a carrier, provided that they do that with the knowledge of the intended recipient.

We do not see how the explanatory memorandum can be correct in that regard, because the Telecommunications Act 1997 states that enforcement agencies need a warrant. We really are concerned about that because, as this committee would be aware, there have been instances in the past where various government agencies have had differing views about what kinds of

warrants they needed or what they were able to do. We really do believe that there needs to be clarity between the interception act and the Telecommunications Act in this regard.

We have made a number of recommendations about improvements for the stored communications bill but I will not go into those at the moment. The other two principal issues we have are with the so-called B-party provisions. We are completely opposed to those. We are also highly concerned about the so-called equipment based interception warrants. We believe that the provisions of the schedule of the bill referring to equipment based interception warrants are largely incomprehensible because most of the telecommunications numbers refer to telecommunications services not telecommunications devices or equipment. Therefore, we simply do not see how these proposed provisions can possibly work.

We also have major concerns in that we do not believe any current telecommunications numbers can be used to uniquely identify a telecommunications device and only that device. We referred in our submission to the comments in the Blunn report that state that, even in the case of mobile handsets, the device number is not necessarily unique. We see the potential here for communications of people who are not the suspect to be intercepted at the same time as people who are the suspect. We also believe that those equipment device provisions, since they are so unclear, seem to have the specific purpose of being used for B-party equipment interception. The basic reason we perceive that is that all of the numbers that are being referred to refer to telecommunications services that can already be intercepted with a telecommunications service warrant or a named person warrant. Therefore, we fail to see why one needs an equipment device warrant to intercept the same service. It is quite technical, therefore we believe the end result is a roundabout way of trying to get access to B-party devices under a warrant. We think it is really more about B-party interceptions than it is about the interception of a suspect's calls, internet communications or anything else. That brings to a close the initial comments I would like to make.

CHAIR—Thank you. EFA along with the Law Council and a number of other submitters are not particularly keen on the B-party provisions of the legislation, if I could put it like that colloquially. What you and the Law Council have done is to basically provide the committee with an 'even if' scenario that says: 'We don't want it but if the government is going to persist with it then ...' What are the key safeguards you think would be necessary if the B-party provisions were proceeded with?

Ms Graham—There is the list that we put in the submission. But, given the speed with which this bill has been introduced to parliament and is going through parliament, I am not prepared to say that the list that we have in our submission is necessarily all that might be appropriate, because the B-party interceptions provision, to us, came out of the blue; we did not expect it. I am aware it was briefly mentioned in the Blunn report but I did not really expect it would come through so quickly with the stored communications provisions. We have not had sufficient time to think through the full range of provisions that could be incorporated to improve the situation.

As I say, we do not approve of these provisions at all. One of the only means, we think, of keeping the use of such warrants to a minimum would be to have a public interest monitor involved in the issue of the warrants with a view to minimising the potential number of times that agencies may apply.

We do not feel that the current situation of having a member of the AAT or a judge listening to a one-sided argument as to why an agency should be granted a warrant is at all adequate in the case of B-party submissions—we would question whether it is even adequate in the case of suspects. Certainly, with B-parties, we believe there should be an independent party involved in the issue of the warrant and monitoring the use of the warrant et cetera to try and limit the amount of use of these warrants for fishing expeditions. We would also say that the bill at the moment does not provide any increased protections in relation to B-party warrants. The additional matters that the issuing authority has to take into account are not very much different from the existing class 1 and class 2 warrants to become 'serious offence' warrants.

There are also issues about the copying and destruction of material, particularly in relation to copies of intercepted material. We have referred in our submission to the changes to the act that were made in 2000 which resulted in agencies not having to destroy copies of intercepted product. The Sherman report recommended that that be changed back to the provisions before 2000, but that has not been done. We would say that that would have to be done. It is utterly ridiculous that it is only the original recording of an intercepted call that has to be destroyed and that copies can be kept willy-nilly forever, it would seem.

We also think that the duration of a warrant would have to be reduced dramatically from the proposed 30 days or 45 days in the case of agencies—I think it is 30 days for ASIO and 45 for the different agencies. Whichever way it is, we think that that should have to go greatly down. We would suggest something like 14 days and then there would have to be proof that those 14 days had resulted in information material to the investigation before there was any renewal.

Also, we note that the reporting provisions do not appear to have to be changed if the B-party provisions were enacted. We would say that any warrants for B-parties should be reported on separately to the minister and the parliament because that would be the only way of being able to identify whether there was a lot of use of these warrants or not. They should not be thrown in with all of the other 'named person warrant' reporting requirements. They are the main things that we have come up with in the short time we have had to think about this aspect.

CHAIR—We understand the problem. What about the use of B-party warrants between individuals on an individual protected usually by professional privilege of some sort, whether it is doctor-patient confidentiality or legal professional privilege?

Ms Graham—That is another major issue that we have. We already think that that is a problem with the existing interception warrants. We think it is going to be an even greater problem in relation to B-party warrants because the B-party may cover a lawyer or someone else who receives a great number of calls or other types of communications that are privileged. I think we may have said in the submission—and I hope we did; we meant to—that B-party warrants simply should not be able to be issued against lawyers or other people who have a large number of calls. In our view that would include politicians. It may include accountants. There may be a number of people, but certainly lawyers.

It is ridiculous to think that people would no longer be able to be confident in seeking legal advice because their lawyer's phone was being intercepted. I know there is a remote risk at the moment in that it is claimed that the existing act would allow that, but my understanding is that it is not being used in that way at the moment. Any extension of it, in our view, would have to make very clear that B-parties could not cover lawyers, because there is too much potential for people who are not a suspect and the lawyer who is not the suspect having their calls intercepted.

Senator LUDWIG—Thank you for coming, Ms Graham. We do appreciate the detail which you provide the committee with. At least from my perspective, it is extraordinarily helpful to be able to obtain a submission of such detail from you. It sheds a lot more light on how this legislation is to work—or is proposed to work, notwithstanding your comments. You may not have had an opportunity to look at the Law Council of Australia's submission, but they also raise a view similar to yours about B-Party intercepts. They also indicate, as an alternative, that if the government were to proceed with this legislation then there are safeguards that they would see as a must. You might want to turn your mind to whether or not you agree with those. They seem to be in addition to the points you have raised, and some are the same.

Ms Graham—I would be pleased to do that, and to get back to you. I had to leave Brisbane mid-afternoon yesterday and at the time I looked at the committee's website there were a couple of others added but that submission was not on there. I was not able to access the web last night at the hotel, due to problems with phone lines.

Senator LUDWIG—We got it late too. That would be helpful. I will go back to the matter of stored communications. I note your submission in respect of the sent items. What about drafts that are kept on the computer, or sent items which are not sent? In other words, there might be a fault with the computer: you have sent them and they have bounced back. They would still flick into the sent items folder. They will also come back to you as a 'not sent' item, won't they?

Ms Graham—Yes, that is a very interesting point.

Senator LUDWIG—The question is: have they passed over?

Ms Graham—Yes, that is right. For actual drafts—where you have not pressed the send button, so to speak—I notice the explanatory memorandum says that drafts are not going to be accessible with a stored communications warrant because they have not passed over.

Senator LUDWIG—So they are 3L?

Ms Graham—Yes. There is a question about what will happen if you have sent it and it has come back again and not been delivered to the intended recipient. I had not actually thought of that at the time I wrote the submission. I think it occurred to me yesterday, in reading something else somewhere. It would seem to me that, whether or not it has passed over, it is not accessible to the intended recipient and the definition of stored communications has a list of three or four things that all have to be met. So it would seem to me that, as it is not accessible to the intended recipient, it is not a stored communication and therefore could not be accessed with a warrant.

Senator LUDWIG—That was my understanding. Therefore it would be 3L.

Ms Graham—Yes. On the other hand, I would expect that, as it comes back to the sender in their incoming mail, that copy of it is probably going to be accessible with a stored communications warrant, because the intended recipient of the bounced message is the sender.

Senator LUDWIG—Yes. At the point that it is to return, then—

Ms Graham—It is coming back to the sender.

Senator LUDWIG—And you tick a box in your Outlook to say whether you want that to come back. You can put in rules.

Ms Graham—Can you? I do not use Outlook.

Senator LUDWIG—In others I suspect you can indicate whether or not you want to know if they did not get it.

Ms Graham—Yes.

Senator LUDWIG—The other area—and this is what I worry about, in terms of the argument—is that it is supposed to be technologically neutral. But we keep coming up with these areas where we hope the Attorney-General will be able to provide a definitive answer. Where do you see instant messaging—MSN and the like—falling, between computer and computer, file sharing and peer-to-peer.

Ms Graham—It is a question of whether they are communications that are happening in real time or whether they are actually stored communications. My understanding of instant messaging is that in the normal course of events it is not stored on a carrier's equipment; it is going from one person's computer to another. So my understanding would be that an interception warrant would be necessary to somehow intercept that. The alternative is that police may obtain these new data surveillance warrants and install them on the recipient's—

Senator LUDWIG—That is a different issue again.

Ms Graham—Yes. There was at one stage an issue as to whether an interception warrant or a surveillance device warrant would be required for those kinds of communications. I mentioned the surveillance device warrant because we feel that this bill eliminates that problem because of the clarity as to what is a stored communication. With instant messaging, I would think that an interception warrant would be necessary, but it probably would be interesting to know what the Attorney-General's Department would say.

Senator LUDWIG—Because the definitions have now changed, does the bill pick up pictures and video? Mobile phones are now far more sophisticated than they were in the past, so you might be sending a picture or diagram rather than a text message.

Ms Graham—My understanding is it does because in the interception act there is a definition of communication which refers, if I recall correctly, to all of the things you just mentioned. To me, if the communication covers all of that and a stored communication is the communication that is some other things as well, it would cover those.

Senator LUDWIG—But the definition of stored communication does not include it. You have to come to the definition of a communication, tie them together and say—

Ms Graham—Yes, that would be my assumption.

Senator LUDWIG—as a matter of interpretation, it should have the same meaning throughout.

Ms Graham—Yes, and certainly the definition of stored communication and the definition of communication are in the same part of the act. It is not that one is in one section and one is in a different section. We would certainly think that they are meant to be read together.

Senator LUDWIG—There are a number of issues that you have raised in your submission that I will be taking up with the Attorney-General, so I will not go to those specifically. Perhaps you could explain 3.1.2, 'Definition of accessing a stored communication and "record"', a little further, because the concern in 3.2 on page 9 is:

The Bill (Part 3-3, Div 1) states:

"110(1) An enforcement agency may apply to an issuing authority for a stored communications warrant ***in respect of a person****."* (emphasis added)

The point you are making is that the bill should be amended to require the affidavit accompanying application for a stored communication warrant to set up the name of the person and details sufficient to identify the person. Have I got that right?

Ms Graham—Sorry, I am having some trouble finding the section and keeping up with that.

CHAIR—He is very speedy.

Senator LUDWIG—Page 9. It is an interesting area.

Ms Graham—So 3.2 and stored communications warrants in respect of a person. We cannot see how, in that section of the bill, there is any requirement that the person is named in the affidavit that is given to the issuing authority, nor that the information about the particular telecommunications service has to be provided to the issuing authority. So our concern is: how does the issuing authority come to know who the person is in respect of whom the warrant is being issued?

I am trying to remember whether this is in relation to stored communication, but I think there is another section where it basically says that, if the agency goes to the carrier and the description of the service or something is not sufficient, the agency can provide the carrier with further information. We have problems with the idea that they can get a warrant that does not clearly specify who the person is and what the telecommunications service is and then go along to a carrier. If the carrier says: 'We cannot identify them. There isn't enough about which of our customers it is,' then the agency can verbally tell the carrier something else about who it is that they are trying to execute the warrant in relation to. We believe the actual affidavit and the warrant should have to specify the name of the person and details of the telecommunications service.

Senator LUDWIG—The other area is this. Currently the AFP or legal or law enforcement agencies use 3L. That is the regime that we have at the moment. As I understand it, 3L will still exist for those situations where the person does not know that they have a warrant effectively being sought for a stored communication. If you are the AFP—and forgive me for verballing them—and you then use 3L of the Crimes Act to access a computer or a mobile

handset, you can then access, still using 3L, everything—emails, SMSs and so on and so forth—once the person knows what you are doing, which is effectively so if they are sitting at the computer or have reasonable notice. Is that still in existence? So that is not going to be moved into the stored communications regime and the stored communications regime will only be where it is an access to an ISP. Have I got that right?

Ms Graham—That is basically my understanding. My understanding is that is certainly so if the communications had been downloaded onto the computer in the suspect's premises and the suspect was also in the premises and had been told that this was being done and therefore had knowledge. My understanding is that the AFP would certainly be able to access communications that were automatically being delivered to that computer at the time that they were searching. If they switched on a mobile phone and SMS messages automatically arrived on the mobile phone, they would be perfectly able to lawfully read them. My interpretation is that they would not be able to use a person's password to log onto the ISP system remotely and intentionally download emails that were stored on the carrier's equipment. That is open to question, but that is my interpretation from reading the provisions of the bill and the explanatory memorandum. I think the intention is that, if the messages are automatically arriving on the equipment without the AFP taking any proactive action to make that happen, then there is no prohibition on their reading them, because those messages are stored on the end user's equipment. But I think there is a quite different situation if they have to use the telecommunications system to log onto an ISP system and then make the messages come from the ISP system over the telecommunications system—

Senator LUDWIG—A different send and receive.

Ms Graham—Sorry?

Senator LUDWIG—In other words, if you press 'send' and receive you are then downloading the messages.

Ms Graham—Sorry, I am not meaning that. It probably depends on which software packages they are. It is the same old story but, yes, it is if they were purposely doing something on the computer to make messages be delivered to it that would not automatically be delivered. There is this issue that with most software packages you can have them set up on your computer so that they will keep on coming through or so that each time you want to access them you have to type in the password so that they will be downloaded. That is where I think the difference is. Say the police come to your computer and they find you have got your password stored on the computer or you have got it stuck on a yellow sticky note, which of course you should not do but people do it. My view is that if they are going to obtain your password and then log onto an ISP system that would be in breach of the stored communications provisions, because they would be accessing the communications on the carrier's equipment.

Senator LUDWIG—What if—say, with Telstra—you used 101? What if you dialled 101 and accessed the voice mail with the handset?

Ms Graham—I would say that that is also not permitted under 3L, because they are actually dialling in. If the messages were sitting on your—

Senator LUDWIG—Yes, if you had scrolled through the handset because there were text messages or if they were already downloaded—

Ms Graham—If they are already downloaded or if they are automatically coming there, then I think they are going to be able to access with 3L. It is if they have to take specific action to make the messages arrive on the end user's equipment. That would seem to me to be not contemplated by the bill.

Senator LUDWIG—It is a fine line.

Ms Graham—Again, this is the fine line. We do have a section about that in this submission, stating what our perception is. But, again, we do feel that that is something that should be clarified so that we do not find later on that the Director of Public Prosecutions and the Solicitor-General again have a different view on what this bill means.

Senator LUDWIG—Or the AFP, for that matter.

Ms Graham—Yes. That is really what I meant—one was the Attorney-General's adviser and the other was the AFP's adviser.

Senator LUDWIG—As I understand the issue with the notice to produce—please correct me if I am wrong—it is where the notice to produce might be subject to the stored communication prohibition. Ultimately, they cannot use their notices to produce where it is a stored communication because there is a prohibition unless you have a stored communication warrant. ASIC, APRA or anyone who can use a notice to produce would want to continue to use a notice to produce and say that the stored communication prohibition does not prevent them from using a notice to produce to obtain the same information. Whereas, you say that it would. There is a specific prohibition.

Ms Graham—Yes—in the Telecommunications Act 1997, which has existed since 1997 completely separate from the Telecommunications (Interception) Act, and there is no indication that there is any intention to change that. Apart from the issue of privacy in relation to this and whether agencies should be able to use a notice to produce, there is also the very serious issue that section 280 of the Telecommunications Act that I am referring to is an exception to the prohibition on disclosure by carriers. If carriers disclose information in breach of that act—in other words, if they disclose information where there is not a specific exception applicable to that circumstance—they are subject to criminal and/or civil remedy proceedings, much the same as under the Telecommunications (Interception) Act.

We feel there is also a serious issue here for carriers—they need to know under what circumstances they are permitted to disclose information. A carrier at the moment would be most unwise to disclose content of communications without a warrant under section 280 in response to a notice to produce because section 280 seems to quite clearly say that if it is an enforcement agency a warrant needs to be provided to the carrier. If they disclose in response to a notice to produce, whether or not the DPP would prosecute you still have the situation that the user may take civil remedy action under the act against the carrier. Not only for the purposes of certainty for users and enforcement agencies as to what the law actually says, there is also this issue of fairness to carriers. They need to know what they can and cannot do.

Senator KIRK—Thank you, Ms Graham, for your very technical submissions—they are most useful. I am interested in the issue of the ability of the Commonwealth to ensure that state and territory agencies actually comply with the legislation. That is an interesting issue. I have read what you have said but could you outline it for us and explain what you think?

Ms Graham—It is basically that under the interception warrant regime that has existed for many years it was apparently necessary for the Commonwealth to require state governments to enact complementary legislation covering their agencies in relation to dealing with communications, destruction of them, recording procedures, reporting and so forth. It was always said that that was necessary because the Commonwealth did not have power over state government agencies. What seems to be happening here is that the government is proposing to bring in extensions to the act to cover stored communications and to grant the power to state agencies, including a very much larger range of agencies than those who can get interception warrants, to obtain a stored communication warrant.

There is nothing in the bill to indicate that state governments are being expected to update their interception acts to complement the Commonwealth act in record keeping, reporting and so on. It is simply not clear to us at the moment how the Commonwealth government, in granting these vast powers to state and territory agencies, can ensure that those are enforced. Given it was perceived necessary to have legislation on interception warrants, why is it not necessary to have legislation in relation to stored communications warrants? We just do not understand that.

Senator KIRK—Yes, it is a problem, isn't it, because, as you say, the obligations on the agencies will not be enforceable.

Ms Graham—That is it. It does not appear to me that they will be, unless there is some aspect of this that we have overlooked that the Attorney-General's Department knows about.

Senator KIRK—We will ask them about it, but it may just be an oversight. Would it be remedied just by enacting a similar provision to what is in the existing legislation?

Ms Graham—Yes. Basically, it would seem to me that the states really need to enact provisions largely similar to the stored communications provisions. Whatever is in the Commonwealth act in dealing with reporting needs to be reflected in state legislation, which is how the interception legislation exists. It seems there would be some issue with trying to get all of the states and territories to do that before 15 June.

Senator KIRK—It is a very short timetable.

Ms Graham—Yes.

CHAIR—Not as short as yesterday's.

Senator KIRK—That is true. It was 14 April, wasn't it?

Ms Graham—Nevertheless, whether it can be done before 15 June or not, it certainly seems to us that something more needs to be done to ensure enforceability by states. By that I mean that we do not want to see this bill delayed because of the current vast access without suitable oversight. It is our view that there is a need for the Commonwealth legislation on stored communications provisions to come into force at the earliest opportunity. But if there is a need for state legislation and it cannot be implemented before June, it seems to me that the

Commonwealth should still do that, even if that aspect of enforceability does not come in until a bit later on after states have had time to update.

Senator KIRK—So there would be that gap for that period?

Ms Graham—Yes, which would still be better than the current situation where they do not necessarily have to get a warrant at all, depending on who the agency is and what they are doing. It is a bit of a staged process to get to the ideal situation.

Senator KIRK—You also mentioned that consideration ought to be given to amending the definition of enforcement agency to:

> ... exclude an agency specified in the TI Regulations from being able to obtain stored communications.

Is that like a stopgap measure?

Ms Graham—It was a kind of stopgap measure or just a thought that we had that, at the very least, if there is not going to be complementary state legislation it would be appropriate to give the minister the power to remove from state or territory agencies the right to get a warrant under the Commonwealth Telecommunications (Interception) Act. It would perhaps be some sort of stick that could be used to make agencies comply. I am not suggesting that it is at all the ideal measure. There would also be the question of whether the minister would in fact feel it appropriate, depending on the circumstances, to use the power, but at least, it would seem to me, it would be an option if it becomes apparent that one state's particular agency is going off on a tangent, doing completely the wrong thing. It was the only thing we could think of that might help at the time.

Senator KIRK—Thank you. We will raise that with A-Gs.

Senator STOTT DESPOJA—Good morning, Ms Graham. Thank you for the quite specific recommendations throughout your submission. I want to ask you about notification of individuals in relation to warrants. Your recommendation obviously says that if we are not pursuing that path as recommended by the Barrett report, what about a public interest monitor. You refer obviously to the Queensland model. Can you elaborate on that? What is your preferred position and what would you like the committee to adopt in relation to those recommendations?

Ms Graham—Really, our preferred position would be that both of those apply: that there be a public interest monitor involved in the issue but that also individuals be notified, say, within 90 days after the execution of the warrant. I really have not had time to look into the details of what the Barrett recommendation was on notification to individuals. If I recall correctly, it was on the basis that it only needed to be done if the warrant did not result in charges against the individual, which would seem to probably be an appropriate situation: minimising the number of times that agencies would need to actually take action to make specific notice to the individual.

From our perspective, the aim of notifying individuals is to put a brake, basically, on the number of applications that could really be fishing expeditions. If there is a requirement that they notify individuals, if the individual is not charged and their communications have been accessed, obviously that would then give any such individual an opportunity to raise issues if

they believed that their communications should not have been accessed. If they feel that the warrant was wrongly issued or whatever, at least they would have an opportunity to take the matter to the Ombudsman or wherever may be appropriate. Whereas the situation when there is no notice is, of course, that there could be many individuals' communications being intercepted, the information is not used and no-one knows about it, so it is not possible to raise questions about whether warrants are being inappropriately issued.

Senator STOTT DESPOJA—Thank you.

CHAIR—Thank you very much again for your submission from EFA. We understand the time frame is a challenging one. We are working with the same time frame.

Ms Graham—Yes, I am aware you are.

CHAIR—We particularly appreciate the detail and the technical aspects of your submission. If there is anything further which we need to pursue with you, we will do that on notice. Thank you very much also for appearing today.

Ms Graham—Thank you very much for having us here.

[10.58 am]

INMAN, Mr Keith, Director, Enforcement, Australian Securities and Investments Commission

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

CHAIR—Welcome. ASIC has lodged a submission with the committee which we have numbered 13. Do you need to make any amendments or alterations to that submission?

Ms Macaulay—No.

CHAIR—I will ask you to make an opening statement and at the end of that we will go to questions from members of the committee.

Ms Macaulay—Thank you for the opportunity for us to appear before this committee. In our opening statement there are two aspects that we would like to raise. The first is to give an outline of ASIC's role and the use to which it puts emails in its investigative and enforcement work, and the second is to outline some issues with the drafting of the current amendment bill.

As you are aware, ASIC is an independent Commonwealth agency. It regulates corporations and it is the disclosure and consumer protection regulator for financial markets and financial products. ASIC considers the use of emails and voicemail is even more common in this area that it regulates than in the wider community. For example, the legal or illegal sale of many financial products takes place using email over the internet. Providers of financial services use email to correspond with their clients and with suppliers of financial products. Officers of a corporation are also frequent users of emails within the corporation and to their advisers. In fact, email has replaced many other forms of communication.

Whereas previously it was a hard-copy document, a letter or a memorandum, it is now an electronic copy document. That exposes a fundamental concern we have with the policy behind this amendment in relation to emails. Given the prevalence of emails and the way that they have overtaken physical forms of documents, we are not clear about why they should be treated differently to a hard-copy document. This is the effect that this bill has. Examples of situations where email would be central to the sorts of misconduct that ASIC may investigate include a suspected wrongdoer sending to another person a spreadsheet by email which contains evidence of funds which have been raised through illegal fundraising or a person may receive an email soliciting moneys to invest in an illegal investment scheme. It may well be that the correspondence by email is the only evidence available to assist us in investigating the misconduct that we are responsible for regulating.

Our regulatory powers cover a wide ambit not only in terms of subject matter but also in the way they operate. We have criminal, civil penalty, civil and administrative remedies available to us. We use all of that those, and we use them very often in combination. Of course, we consult with the Commonwealth Director of Public Prosecutions before charges are laid, and they pursue the prosecutions. We do our own civil penalty and our own civil proceedings. We also do a lot of administrative proceedings, particularly in relation to regulating management of corporations and financial advisers.

We have extensive powers to serve notices to obtain material, both physical and electronic material. We also make use of search warrants under the Crimes Act where that is necessary and we have a search warrant power in the ASIC Act, which is available where we have served a notice and the notice has not been responded to. The notices that we serve are not prospective—that is, they cannot seek material that is not currently in existence; they only seek material which is in existence at the time the notice is served. To this extent, they do not allow access to real-time data—that is, they do not allow access to data as it is being created.

Under the current provisions that are enacted in relation to stored communications, we can access stored communications that are in existence and are held by a carrier which have not been accessed by the recipient or which have been accessed by the recipient but are not in the recipient's possession. We cannot do that covertly to the extent that we cannot get real-time access to it. It is only to material that is in existence. In some cases the legislation that is contemplated will make the investigation and prosecution of fairly serious contraventions of the financial sector law impossible. That is because of the need to seek a search warrant if we are going to access stored communications held with a carrier. There is a threshold which relates to the ability to obtain a search warrant. In many cases, the provisions of the Corporations Act will not meet that threshold. That will affect our ability to collect evidence of misconduct.

The specific issue we have with the draft bill in its current form is the threshold for obtaining the warrant—three years or 180 penalty units. We have many examples of provisions throughout the Corporations Act which address serious misconduct which have a lower threshold than that. For example, a person who is disqualified from managing a corporation may be prosecuted if they continue to manage a corporation. That is only a two-year penalty. There is an offence if a director of a listed company fails to disclose a relevant interest. That also falls below the threshold. There is also a range of offences in relation to defective product disclosure documents for financial products. They all fall outside the threshold to obtain a warrant.

Once material has been obtained under a warrant, there is a slightly broader category of material for which it can be used, but it still does not cover a lot of the remedies that we seek. It does not cover any civil remedies that we might seek—injunctions to stop conduct or to freeze assets. It does not cover any administrative proceedings that we might take to exclude financial services providers from the industry. Our civil penalty provisions allow us to seek a combination of three remedies. We will not be allowed to use stored communications warrants material to seek compensatory remedy or a banning remedy for a civil penalty. We anticipate that the legislation intends that we could seek a warrant for a civil pecuniary penalty proceeding. But, as it is currently drafted, the monetary equivalent of a pecuniary penalty does not refer to Commonwealth legislation; it only refers to state or territory legislation, so there is a bit of a gap in that regard, which we assume is inadvertent.

Mr Inman—Madam Chair, may I reserve the option to make a few comments from an operational perspective before we conclude?

CHAIR—Absolutely.

Mr Inman—Thank you.

Senator LUDWIG—Let me understand the process. Notice to produce is an old power that ASIC had, and a range of other quasi criminal actions. It was originally about gaining record books, types of records, paper based computer printouts and that type of information that was available that you needed to obtain to then assist in a civil case, a prosecution or a quasi criminal case if a sanction applied. You now use modern technology. Where do you stop? If you use a notice to produce, do you currently produce it to the ISP?

Ms Macaulay—That option is available to us under the current legislation.

Senator LUDWIG—You then issue a notice to produce to a particular ISP concerning a corporation or a company that you have a particular interest in and the relevant email addresses of the corporate heads that you might be interested in? There might be Mr Bloggs and so on.

Ms Macaulay—Yes.

Senator LUDWIG—You then go directly to the ISP and ask, 'Can you provide a printout or a copy or a data disk of all the email traffic that has gone from A to B to C?' Is that what you do?

Mr Inman—We have done that in the past. The majority of our access to emails, however, comes from access at the user's end, whether that be a company—

Senator LUDWIG—I was going to come back to that point. I was just exploring this end, then I will come back to that.

Mr Inman—I just wanted to convey a feeling that we have done that in the past, but the majority of our access is at the other end.

Senator LUDWIG—The ISP is not under an obligation to notify the corporation that you are investigating and neither are you with the notice to produce to the ISP?

Ms Macaulay—That is correct.

Senator LUDWIG—In fact, you do not want to notify them, because you might be covertly examining their emails for a breach of the TPA under collusive tendering and whatever?

Ms Macaulay—I would not use the word 'covertly'.

Senator LUDWIG—If you don't tell them, what do you call it?

Ms Macaulay—There is nothing to prevent someone disclosing whether or not they have received a notice. We very often serve notices on parties. Our notices require parties who have received a notice to serve the documents that are in their possession and that may well include documents that are third party documents. For example, we routinely serve notices on banks and ask for details about clients of the bank and particular cheques that we may need as evidence of misconduct.

Senator LUDWIG—But when you serve the notice to produce on an ISP in relation to a corporation and individuals, do you then send a copy to the individuals?

Ms Macaulay—No, and we do not when we serve a notice on a bank, either.

Senator LUDWIG—It has to be covert then. Forgive me if I do not understand but if you do not tell the intended recipient—

Ms Macaulay—That is true. There are many instances where we would prefer a third party, whose documents may be held by the recipient of the notice, not to know because if they do know and they understand that we are doing an investigation then they may take action which will affect our investigation.

ACTING CHAIR (Senator Ludwig)—They may take out an injunction—

Ms Macaulay—Yes, there are many different sorts of actions.

ACTING CHAIR—to stop you doing it?

Ms Macaulay—Yes.

ACTING CHAIR—So it is covert—you do not want to tell them? This is not a trick question.

Ms Macaulay—No. The use of the term has certain connotations which we would not agree with.

ACTING CHAIR—But that is what you are doing. If that is what you are doing, why do you have a problem with the term?

Ms Macaulay—There is no prohibition on disclosure of the notice. 'Covert' gives a flavour of secrecy.

ACTING CHAIR—Hang on a minute—let us deal with secrecy then.

Ms Macaulay—There is no obligation on someone to keep secret the fact that they have received a notice.

ACTING CHAIR—Are you sure about that?

Ms Macaulay—Yes.

ACTING CHAIR—Under your legislation?

Ms Macaulay—Yes.

ACTING CHAIR—What about other legislation—the telecommunications legislation or the telecommunications interception legislation?

Ms Macaulay—We do not have any powers under the telecommunications interception legislation.

ACTING CHAIR—You do not know whether it prohibits that? I will not explore that. In terms of 'secret', though—we can use that term if you are more comfortable with that—you do not tell the intended recipients, so therefore it is secret.

Ms Macaulay—Right enough—we do not tell them. There is no obligation to make it secret.

ACTING CHAIR—No—as far as you are aware.

Ms Macaulay—I can tell you categorically that there is no legislative prohibition on the recipient of a notice disclosing that notice.

ACTING CHAIR—We will ask the Attorney General's Department that question later and see what they say. Your objection is that a stored communication regime will mean that you will have to seek a warrant for the information that you are currently able to access. Will it place impediments or difficulties on you? What is the problem that you would perceive?

Ms Macaulay—A warrant is available only in certain circumstances. You need to meet the threshold, that it is either—

ACTING CHAIR—Yes.

Ms Macaulay—And many of the types of misconduct that we pursue will not meet that threshold. That means that we will not be able to access that material during the course of our investigation and that will affect, to a varying degree—depending on what the information is—our investigation and our ability to assess whether or not misconduct has occurred and then our ability to take action if it has occurred.

ACTING CHAIR—In respect of accessing information that the recipient might have—for argument's sake, on a computer in an office environment; we can use that as an easy one to imagine—you can serve a notice to produce and then ask for the email traffic that is stored on that computer, that is passed over and that is available?

Ms Macaulay—Yes.

ACTING CHAIR—Could you also retrieve and take print-outs or copies of the sent items, drafts and anything else on that machine, in relation to email traffic?

Mr Inman—It all depends on how the machine has been set up. It is possible that there will be nothing on the machine. So we can get either all of that or nothing, depending on how the machine has been set up.

ACTING CHAIR—So if the computer is set up with a send and receive button, can you press that in your investigation, with a notice to produce, and ask them to then download from the carrier that information—the last email traffic that might have come through? I am not too sure how your investigation might operate.

Mr Inman—It depends. We have the ability to require people to provide reasonable assistance. It is arguable whether or not we could use that means to require someone to press the send and receive button. If we have entered the premises under a search warrant, we have the 3E and 3L provisions.

ACTING CHAIR—So you use 3L where you see people taking data away from computers. You use that as a basis. Your notice to produce is a slightly different version of the 3L?

Ms Macaulay—Yes, that is right. We routinely use notices to produce. We literally serve thousands of them every year in different contexts—some are for compliance and surveillance purposes and there are investigative purposes as well. We use search warrants only when we have an apprehension that evidence may be lost. The key thing about our notices is that they apply to books, and that is a defined term in the ASIC Act. It covers electronic material as well as physical material.

Senator LUDWIG—Have you raised those concerns with the A-G's Department?

Ms Macaulay—Yes, we have.

Senator LUDWIG—What was their response?

Ms Macaulay—They listened to it; they understood it; they have not given us a response yet.

Senator LUDWIG—So we might hear from them this afternoon as to what their response might be.

Ms Macaulay—Yes, you might.

CHAIR—They might be busy talking about other things.

Senator LUDWIG—Yes. Have you asked whether or not they will provide a response to you?

Ms Macaulay—My understanding—and I have not spoken directly to the Attorney-General's Department, but I am informed by my officers—is that we have not directly asked them that question. We have had a number of discussions with them and we have an expectation that they would respond to the issues that we have raised.

Senator STOTT DESPOJA—I have a general question. I found your introductory remarks in your submission with regard to the impact that the legislation would have on your work quite interesting. Can you further outline and even quantify—and I am not sure if that is possible—what you perceive the impact of this legislation will be on your work and outcomes, particularly in relation to civil and administrative proceedings when it involves those particular forms of remedy? Is it possible for you to explain what you think will happen?

Mr Inman—I can do two things. One is to give a general comment and the other is to give an example of a specific impact.

Senator STOTT DESPOJA—That would be helpful.

Mr Inman—We believe generally that things that we can currently gain access to for a whole range of investigations will be narrowed as a result of this legislation, because there are lots of penalty provisions within the legislation that we administer that are less than the threshold being set at the moment or that are being discussed for the three years or 180 points. Obviously, that removes some tactical advantage from us in our investigations and some practical access. We perceive we will not be able to get certain information as a result of that.

I can give you a specific example. The example I am about to give is based on our operational experience in the past where we have relied on serving notices or obtaining from intermediaries like an ISP some email traffic. I can imagine a situation where a consumer complains to us about an unsolicited offer that they have received. We look at this and it appears that it has come from someone whom we may have banned previously. However, a single email containing an offer as an attachment would not be sufficient proof for us to do anything other than suspect there may have been a contravention of that banning order. What we would normally do in that situation, because we would know who the person is, is serve them with a notice. We would probably serve them with a notice and ask them to give us a copy of their computer. We would image their computer. I can remember situations that have

occurred in the past where, because of the way the computer is set up, we did not find not only an example of the email that was sent but any other emails. There may be only a few remnants of some non-related emails. We examine the individual and we say to them, 'Can you explain this email?' They say, 'I don't remember sending it.' Because the contravention of a banning order is less than that threshold, we have no means to test the veracity of the evidence that we have been given. If we could go to the ISP, we could possibly see replies that that individual has had from other prospective investors. That will not be available to us if the bill goes through in its current format.

Ms Macaulay—I just add that we would not as a matter of course go to an ISP as our first port of call to seek to access this sort of material. Normally, we would go to the recipients of the information or the senders of the information in the course of gathering together a whole lot of material which will enable us to understand what the particular transaction or course of conduct involved. The situation that Keith outlined is a situation where that information is not available from these other sources. That is when we would go to an ISP.

Senator STOTT DESPOJA—That is fine. Thank you.

Senator LUDWIG—With regard to the low order of types of offences, are they all pecuniary offences for which you use notices to produce, or can they be non-pecuniary offences?

Ms Macaulay—They can be non-pecuniary. There is a whole range of potential remedies. We might have an investigation that is criminal, and we would use the notice to obtain material for that, or a civil penalty, or an injunctive proceeding or an administrative penalty. We would very often do an investigation which had a combination of things. We may think that there has been an offence committed, but, at the same time, the person holds a financial services licence and we would be considering whether or not they should be banned from the industry. We may also want to know whether or not we need to seek some injunctive action to restrain illegally raised funds.

Senator LUDWIG—If this regime is implemented by the government, how will that impact upon your investigatory work and your ability to be able to oversight corporations and do the work you do? Have you been able to make some assessment of that? You will have one area that you will not be able to access.

Ms Macaulay—Yes, that is correct.

Senator LUDWIG—You will have one area where you will only be able to access under a stored communication warrant.

Ms Macaulay—Yes, and then only in certain circumstances. As I said, the ISPs are not our first port of call. We do not routinely go to them, so it would be a limited number of situations where we would say, 'Do we need to go to an ISP, and can we meet that threshold for getting a search warrant?' But I can say that it is a real likelihood that those situations will arise.

Senator LUDWIG—You might want to take this on notice, but I would not mind finding out the number of times in the last 12 months or so that you have accessed ISPs for that type of information, for both pecuniary and non-pecuniary penalties.

Ms Macaulay—Yes.

Senator LUDWIG—It would be helpful, thank you.

CHAIR—It would indeed. Mr Inman, did you want to make any further comments in relation to those operational matters?

Mr Inman—If I may, but only to add a further explanation regarding our reluctance to use these terms 'covert' and 'covertly'. At the moment, the connotation attached to these terms, as they appear in the TI Amendment Bill, relates to covert access in the same way that we would refer to police accessing or tapping a telephone call. Our position is that the impact of this bill is not only going to deal with contemporaneous conversations but it is going to impact upon documents that are emailed, and there may be no text in the email other than, 'Have you seen this?' Or there may be nothing, because the offer itself is the document or the document may be an Excel spreadsheet they have seen.

In our world, we are providing notices to third parties, as Louise has said, obtaining thousands of documents over a period of a week. Most of those documents have an element of confidentiality attached to them, and many of them probably fall within the definition of a private record under the Privacy Act. We do have obligations across a whole raft of legislation to protect the confidentiality and the privacy of that. I can think of our own legislation, I can think of the Crimes Act, I can think of the Public Service Act, I can think of the Privacy Act. We deal with those obligations very seriously every day and every week in relation to thousands of documents. That is how we perceive we are operating. We do not notify every affected party in those thousands of documents that we obtain from an intermediary, not because we perceive that we are operating covertly, but because that is how we access information. That is the only additional information I would like to add.

Senator STOTT DESPOJA—I have a very quick query. Have you discussed any of your concerns with the ACCC?

Ms Macaulay—No, we have not, but I have read—

Mr Inman—I think we have, through the AGEC forum.

CHAIR—As there are no further questions, Ms Macaulay and Mr Inman, thank you very much for your attendance and thanks to ASIC for your submission.

[11.25 am]

CLAPIN, Dr Hugh James William, Deputy Director, Policy, Office of the Privacy Commissioner

PILGRIM, Mr Timothy Hugh, Deputy Privacy Commissioner, Office of the Privacy Commissioner

CHAIR—Welcome. The Office of the Privacy Commissioner has lodged a submission with the committee which we have numbered 6. Do you need to make any amendments or alterations to that submission?

Mr Pilgrim—There are no alterations. There might be some other points in my opening comments.

CHAIR—I invite you make an opening statement and then we will go to questions.

Mr Pilgrim—Thank you for the opportunity to appear before the committee. The Office of the Privacy Commissioner recognises that telecommunications interception activities, by their very nature, intrude on the privacy of individuals. This has been acknowledged by the drafters of the bill and also in the review of the regulation of access to communications undertaken by Mr Blunn last year. However, we also recognise that the community expects that law enforcement agencies will have access to appropriate tools to allow them to efficiently undertake one of their key roles in the community—that of investigating criminal activities. The challenge facing the community is where to strike the right balance between these important community priorities. Is the response, for example, proportional to the risk that has been identified? This, in itself, is a difficult question for our office to answer, partly as we do not have a regulatory or monitoring role under the act and therefore do not deal with the provisions of the interception act on a day-to-day basis.

In our submission we comment on four aspects of the amendment bill. Firstly, stored communications: in respect of this, we acknowledge that the amendment clarifies the regime for accessing stored communications. However, we note that it also provides for agencies such as the Australian Taxation Office, Customs, ASIC and similar state and territory agencies to have access to warrants under the interception act for the first time. Given that, it is important that there are suitably robust reporting requirements in the bill to ensure a level of transparency and ongoing monitoring of the stored communications regime.

Secondly, B-party interception: it is clear that B-party interception may significantly increase the likelihood that communications that are not relevant to a specific investigation will be collected by enforcement agencies. In this regard, we acknowledge that there are specific protections included in the bill such as these interceptions being undertaken as a last resort and being subject to shorter warrant periods. However, we believe that there could be stricter parameters around the use and disclosure of information collected under these warrants, including enforceable prohibitions for using this information for any purpose other than that stated on the warrant. Further, we believe that there should be immediate destruction of irrelevant material collected through these interceptions.

Thirdly, equipment based interception: the office has not been able to fully determine the limits of the operation of equipment based interception. While we can appreciate that

intercepting a mobile phone handset on the basis of a handset itself may provide a practical solution to the problem where individuals may use many SIM cards in the one handset, the provisions in schedule 3 appear to go beyond that scenario—for example, in permitting equipment to be identified on the basis of an email address or a user account identifier. These would not normally be thought of as equipment identifiers but, rather, as identifiers of a telecommunications service, and the existing provisions of the interception act already permit the interception of telecommunications services. It is therefore unclear to our office what the effect of these provisions will be, and we believe there should be careful consideration given to ensuring the provisions of schedule 3 do not give rise to an unintended reduction of the privacy protections in the interception act.

Finally, in respect of section 6(2) of the act: the office supports the repeal of this section as in the past it has given rise to confusion in respect of the circumstances under which phone calls may be covertly monitored.

These provisions mark significant changes to the framework for accessing telecommunications, giving rise to greater collection, storage and handling of private communications. As such, we believe that, to support the mechanisms already in the bill that provide for reporting and monitoring of these activities, there should also be a formal review process on the operation of the Telecommunications (Interception) Act. This could, we believe, be included in the current bill. Thank you, and I welcome any questions from the committee.

CHAIR—Thanks very much, Mr Pilgrim. Dr Clapin, did you wish to add anything at this stage?

Dr Clapin—No, I do not.

CHAIR—On your concluding point on the review process, Mr Pilgrim, how would you envisage that working?

Mr Pilgrim—There are probably a couple of ways in which that could be done. There could be a further amendment made to the amendment bill which could put into place a statutory requirement for a review of the interception act. There could be an undertaking given by the Attorney-General through his department for a regular review process. Having said that, I note that in Mr Blunn's report, which I referred to earlier, he in fact acknowledges that there is a possible need for an ongoing review and, I think, points out a period of approximately three years. I think our office would support a three-yearly review of the ongoing operations of the act.

CHAIR—You make, in your submission, some observations about the potential need for stricter parameters around the use or disclosure of material collected via B-party interception warrants based on a premise that if we go down the road of B-party warrants then a lot of material is going to be collected which is not relevant to the investigation. You raise some concerns about the method by which material should be dealt with, stored, moved to destruction and so on. How do you think we can tighten that process up to make sure irrelevant material is destroyed expeditiously? In fact, you raise a similar concern about stored communications, but I will come to that in a moment.

Mr Pilgrim—I suppose what we are looking at is a tighter reference to, particularly, the destruction of information. My understanding, and Dr Clapin may be able to add further detail, is that the destruction is basically around when there is no longer a relevant use for that information. It is hard to determine when that decision point may come, when a particular enforcement agency may be able to, if I could put it bluntly, get around to examining the information and making that decision. It runs the risk that you could have large amounts of, as we say, irrelevant information sitting around in agencies, which does ultimately lead to a risk in terms of security and in how that information is going to be stored and handled. We probably could suggest that time frames might be one way of putting a bit more specificity into the provisions, but acknowledging that it is often very difficult to determine an appropriate time frame.

CHAIR—You suggest audited requirements that any intercepted material outside the scope of the purpose stated in the warrant be immediately destroyed. Should they be audited by the Office of the Privacy Commissioner—who did you have in mind for that role?

Mr Pilgrim—I am certainly not suggesting that it would necessarily be our office that would be undertaking that role. That would be a move away from the current regulatory role of our office with regard to TI, which is no regulatory role. It could be that, for example, the Ombudsman, who does have some regulatory roles under the Telecommunications (Interception) Act, could perform that sort of a role.

CHAIR—The poor old Ombudsman is already slightly apprehensive, it is fair to say based on his submission, about what he is going to be required to do under the bill as it is structured unless his office is adequately resourced for that.

Mr Pilgrim—I can sympathise with that.

CHAIR—We could make Professor McMillan's day by adding that to the list! But I understand the point that you make and I think it is important. On the question of stored communications, you also suggest that the way the bill is structured we may end up with the effect that it would be lawful for an agency to keep irrelevant information indefinitely. I think your suggestion is that it would be possible to amend the bill to ensure that agencies are required to take steps to regularly review whether the information they have accessed via stored communications warrants is still required for a permitted purpose. I think you suggest a maximum period for review. That is a standard approach for good privacy practices, as I understand it. Is that a reasonable interpretation?

Mr Pilgrim—It is a reasonable interpretation. Specifically, in the national privacy principles, which cover the private sector, there is reference to organisations regularly ensuring that the information they hold is not kept unnecessarily and is deleted as soon as it is no longer required. It is a standard practice or understanding in much of the privacy legislation around the world that information can become out of date, for example, if it is not being used and not being updated, and therefore not necessary or useful to an organisation. The risk here, of course, is that lots of information about people who are not necessarily people of interest in a particular investigation is potentially likely to be held by a large number of organisations. The questions are: what is going to happen to that information when it is in those organisations; who is going to be able to get access to it in those organisations

and see it; and if it is inadvertently disclosed what damage is it likely to cause to the potentially innocent third party who may not be the subject of the investigation?

CHAIR—In relation to stored communications, you make the point that we have to get to a stage where the chief officer of the relevant agency is satisfied that the information is not likely to be required for the purposes of subsection 139(2). That presupposes that the chief officer has the time to do that in relation to the quantum of material that is collected under this process.

Mr Pilgrim—That is right. It is not necessarily a responsibility that should fall entirely onto the chief officer. One would assume there would be an ability to delegate some sort of powers but, nevertheless, the ultimate responsibility should be on the chief officer of a particular organisation to be responsible for what happens with the personal information that they are holding at any time. For example, under the Privacy Act at the moment, the organisation and its chief executive officer are ultimately responsible for anything that happens against the provisions of the Privacy Act within their agency. It is not necessarily the responsibility of an individual officer who might be undertaking a particular piece of work at that time but it is the responsibility, ultimately, of the CEO to be responsible for what happens in a particular agency.

Senator KIRK—Thank you for your submission. I want to ask about some of the safeguards that could perhaps be put in place in relation to B-party warrants. It has been mentioned to us this morning and in some of the submissions that perhaps a public interest monitor might have a role in this regard, perhaps even in the process of the issuing of the warrants. I wonder if you think that would be a good safeguard to put in place to oversee this process.

Mr Pilgrim—It is not an issue we have obviously turned our mind to as part of our submission, but a preliminary thought would be that there is already a process in place for the issuing of the warrants through judicial officers or AAT officers and that gives an oversight that the community is probably fairly generally acceptable of in terms of warrants being issued. You then need to ask the question: if we accept that, what is the regulatory role or who has oversight? You then have the Ombudsman, who does have an ability to handle complaints from individuals should they believe some action is being taken to them that has not been in accordance for a warrant, for example. So there is a role there. On the issue of establishing another body, I really do not have a firm position on that. I am not sure whether or not it would be doubling up on one or other of the roles that I have just mentioned.

Senator KIRK—It was mentioned to us this morning by the law society that the very nature of this is that people often do not know that their communications are being intercepted, therefore that perhaps makes it difficult in some circumstances to make a complaint which the Ombudsman can then act upon. There were also concerns expressed that, particularly with the Attorney-General having a role in the issuing of a warrant, perhaps there might be an additional role—I know it is adding another level of bureaucracy—for a public interest monitor to be involved at that early stage, as the warrant is being issued. Perhaps it is not something that you have a view on, but I am thinking of privacy concerns.

Mr Pilgrim—No, it is not something we have a particular view on.

Senator STOTT DESPOJA—Was the Office of the Privacy Commissioner consulted about the drafting of this legislation?

Mr Pilgrim—Our office has had discussions with the Attorney-General's Department on various stages of the development of the legislation. Whether we had definite involvement in drafting legislation I will just check with my colleague Dr Clapin.

Dr Clapin—We were given a draft of the bill at one stage and we made comments on that. I would not say that we contributed to the drafting of it but there were comments on a draft bill.

Senator STOTT DESPOJA—Do you feel that some of your comments have been interpreted or incorporated into it? I assume that you had an exploratory draft and you have given some feedback. Do you see that feedback reflected in the legislation before you?

Mr Pilgrim—I would suggest that we certainly would have made some observations and comments—and, again, Dr Clapin may wish to expand on this—along the lines that we would have expected to see good monitoring and reporting roles and transparency. I note that in various provisions those factors have been included or are in the bill. So at one level I would say that, certainly, some of the issues we raised have been incorporated along those lines of monitoring and reporting.

Senator STOTT DESPOJA—That is good. With regard to the role of the Privacy Commissioner—and I am just teasing this out a little before talking about the bill per se—I am wondering whether there is more of a role for the Privacy Commissioner in terms of this kind of legislation that is being drafted. I am not just talking about this bill in isolation but, obviously, when coupled with the recent antiterrorism legislation and other changes. I am wondering whether you will see the office as having a more formalised role in terms of being consulted or advised when this legislation or comparable legislation that may or may not have an impact on privacy rights is being put forward. Is that something you would care to comment on?

Mr Pilgrim—In terms of commenting on that particular issue, we have welcomed the amount of involvement we have had from the Attorney-General's Department to comment on issues around the Telecommunications (Interception) Act. I say that referring back to my earlier comments that we do not actually have, as I said, a formal regulatory role. So it is obviously perceived by the key stakeholders such as the Attorney-General's Department as an important privacy issue to the point that they do involve us when there are likely to be amendments, without the need for any formal identification of a role for us within the act.

I would also extend that to the recent review that was done by Mr Blunn when our office and the commissioner had several meetings with Mr Blunn and we provided a submission to his review as well. We did not have to actually go and seek those interactions; we were approached willingly to put our views, and we welcome that. I would also point out that within the Privacy Act itself, under the commissioner's functions under section 27(1), we do have a key function to comment broadly on enactments or amendments to bills that have an impact on the privacy of individuals. That is paraphrasing, obviously, but we do have a formal role in our own act to comment on bills.

Senator STOTT DESPOJA—I recognise that you have a role and I am interested in how that actually takes place, how that manifests itself. When you are engaged in such consultations or the proffering of advice or reading legislation or what have you—providing submissions, for example—what impact does that have on the office? Dr Clapin, are you spending most of your time reading and presenting reports or analysing and assessing reports? I am curious from the perspective of resources in terms of the office. Firstly, I do not underestimate your workload and, secondly, I think that everyone in this room is aware of the increasing legislation that has an impact on privacy, for better or for worse, requiring analysis and investigation.

Mr Pilgrim—Naturally, replying to any changes in legislation or providing submissions or comments is going to impact on the office at the resourcing level. In response I would say that we look at the particular issues at hand and at the usefulness of any comments we might have to add on a particular issue and then we prioritise our workload around that. If, for example, it is going to be a key issue that is impacting on privacy, such as the Telecommunications (Interception) Act, we certainly try to make an attempt to be able to provide some commentary on it because it does have a key impact on the collection of personal information. So, without trying to make it sound glib or a short answer, it is a matter of prioritising for us, and we tend to focus on issues when we think we can make the best impact on those issues that are going to have the greatest impact on the community.

Senator STOTT DESPOJA—Dr Clapin, would you like to add anything to that?

Dr Clapin—No, not at all.

Senator STOTT DESPOJA—In your submission you refer particularly to schedule 3 of the bill and say:

> The Office has not been able to fully determine the limits to the scope of the operation of Schedule 3, and so recommends that careful consideration be given to ensuring that the provisions of Schedule 3 do not give rise to an unintended reduction of the privacy protections ...

I was wondering what difficulties you are having in deriving the limits to the scope of that schedule. Is that something you would care to comment on and explain for the committee?

Mr Pilgrim—I will certainly give it a go and then I might hand over to Dr Clapin, because it is an issue that we have been grappling with and, given our time to be able to devote to issues such as this, have not been able to fully explore. As I said in my opening address, it seems that the equipment based interception provisions are looking at identifying and intercepting pieces of information. What we see in some of the definitions is a link through to identifiers that go beyond the equipment itself. An example of that is email addresses.

What we are not able to grapple with—or have not had time to grapple with—is how that might be broadly applied in various scenarios. One scenario I might use—and I do not know whether it is necessarily the best one—could be internet cafes. For example, if you are looking at bits of equipment in an internet cafe and you are looking at the number of people who use those pieces of equipment, what we are not sure about—and, again, there may be a simple answer to this—is whether going in and seeking to access equipment based interception using a person's email address is in some way inadvertently going to allow an enforcement agency to get access to a piece of equipment that is broadly used by large

numbers of the public, such as a piece of equipment in an internet cafe, which will then allow for possibly huge amounts of other people's personal data to be collected. That sounds vague—and I acknowledge that simply because we are basically not too sure about the scenario.

Senator LUDWIG—Are you saying that, if they were only using a web based email address at internet cafes, the only way they could do an equipment based interception would be to do exactly that—use the MAC address of the 15, 10, five or whatever computers that are in that café? Is that the point that you are not sure of?

Mr Pilgrim—I think that is right. I might hand over to Dr Clapin, who might help me out of this quagmire!

Dr Clapin—Or dig myself in deeper.

CHAIR—It is a very shallow quagmire, so I would not worry too much.

Dr Clapin—One question would be whether that would be permitted already under a telecommunications service warrant, with the analogous effect of identifying the telecommunications service, and therefore you do it that way. I think that is one of the questions around the definition in the bill of 'telecommunications number'—where it defines it as a MAC address, an email address and so on. With a lot of those things—user account identifier is another one—it looks more like a service. So it may not broaden the scope of the act or the number of interceptions because these things may already be permitted under service warrants. It just seems an unnatural conceptual fit to be putting these service identifiers as identifiers of equipment. So I guess there is then a question of whether there are consequences that need to be carefully thought through.

Senator LUDWIG—Would it be broader in the sense that the original warrant was for the email address and it would have then been a suspect in the sense that they had particular information that they wanted to gain? But, in terms of an internet cafe with 15, 10 or five MAC addresses, you are then collecting information from nonsuspects and, of course, you then have the issues of storage, handling and destruction of that material and the off-chance that the web mail address is in fact going to be utilised.

Mr Pilgrim—We would say that is a possibility as well, on our current understanding; but, again, we are very unclear and we think it might be worth a question being asked for clarity around that particular issue.

Senator STOTT DESPOJA—I think that is what we will be doing today, because I note in the submission from the EFA, who are also grappling with it, that they suggest that that schedule be deleted. The fact that you are grappling with the scope of that schedule is an indication that we also might have some similar difficulties. Having said that, I note the *Alert Digest* on this bill said:

> ... amendments in this Schedule would appear to trespass on the personal rights and liberties of anyone who happened, in all innocence, to use a computer terminal or mobile telephone handset in relation to which an interception warrant had been issued. The Committee makes no final determination on this matter but **leaves for the Senate as a whole** the question of whether the amendments trespass *unduly* on those personal rights and liberties.

I do not suppose, Mr Pilgrim, you are in a position to say whether or not the Office of the Privacy Commissioner believes that it trespasses unduly on liberties and personal freedoms at this stage?

Mr Pilgrim—That is right. I would say at this stage, because of our lack of clarity around the whole issue, we are just not sure of the extent. It would probably a bit too early for us to comment on something so definite until we were able to see a bit more clarity.

Senator STOTT DESPOJA—You say 'a bit more clarity'. Apart from the clear cut-glass clarity that we will get this afternoon, I have no doubt, will the committee process get some feedback from you, if you have time? High expectations, guys—you know!

CHAIR—Raise that bar!

Senator STOTT DESPOJA—It is all about thresholds today. Is this something that you would seek to provide further information to the committee on, bearing in mind that we have heard evidence today that may go to the workings of that particular schedule as well? We invite you to provide further information, if you like.

Mr Pilgrim—I suppose my answer is that once we have seen any further information that builds on what we already understand then we will make a decision about whether we need to provide any further advice to the committee.

Senator STOTT DESPOJA—Fair enough. Thank you for that. I have a question that goes back to the issue of the parameters to which you have referred, particularly in relation to the B-party interception. You listed both in your submission and verbally here some ideas like the enforceable prohibitions, audited requirements et cetera. Just to make this very clear for the committee, are you suggesting specific amendments that could be made to the legislation in order to build in those protections or parameters so they should be enshrined in law?

Mr Pilgrim—Yes. Without being able to go into the specificity or the wording of them at this point, we would expect to see something else enshrined within the legislation.

Senator STOTT DESPOJA—I have a general question. I am just wondering if you would care to give us an assessment of where we are on so-called privacy rights in Australia today, particularly as a result of legislation that has been passed in recent times? I am wondering about the cumulative effect of this law, antiterrorism legislation and other surveillance based legislation. Do you believe that the passage of these bills has had an impact on people's personal freedom and so-called privacy rights?

Mr Pilgrim—That is a fairly large question and one that it is probably not incumbent upon me to answer on behalf of the commissioner. I can certainly take it on notice to discuss the issue with the commissioner and ask whether she feels she would like to make any comment on that. The only point I would make is one that the office makes generally with regard to legislation of this nature of antiterrorism laws and similar bills, and that is the need to get the balance right to make sure that the response to the risk is proportional to that risk and that wherever possible it minimises the impact on civil liberties. That is a statement we would make with regard to most legislation and I think it is applicable here, as with any other legislation or bill we are looking at.

Senator LUDWIG—In making that assessment in respect of this legislation, do you say that for B-party and equipment based interception and stored communication the balance is not yet right?

Mr Pilgrim—With regard to B-party information, it is clear—as we have said and as I am sure a number of other submitters have said—that it has the potential to collect huge amounts of information from people who are not people of interest, therefore we need to make sure the balance is right. In doing that, where we have identified there need to be some improvements to the bill are particularly around the issue of the destruction of the third-party information. We think that would help get that particular aspect of the bill to a more balanced perspective.

Senator LUDWIG—You say in your submission:

> Such parameters may include enforceable prohibitions on the use or disclosure of intercepted material for any purpose other than the purpose stated in the warrant; and enforceable, audited requirements that any intercepted material outside the scope of the purpose stated in the warrant be immediately destroyed.

Are those the sorts of things you mean?

Mr Pilgrim—That is correct.

Senator LUDWIG—Would you see those as a must, to ensure that the balance is right?

Mr Pilgrim—A must? I would suggest that we would think that they would go a long way to improving the bill and getting the balance right. There may be other options that we have not been able to cover or we have not thought of that may go some way to addressing those issues as well, so I would be a bit loath to state that they are a must, because someone may come up with more effective means for improving that particular aspect of the bill.

Senator LUDWIG—On that point, though, if you have an opportunity in the short time available to look at what EFA and/or the Law Council of Australia say in their submissions in opposition to B-party interceptions, it would be helpful for the legislation—if you could cast your eye over those to see whether or not you agree with any of those additional protections.

Mr Pilgrim—Certainly, we will try to take some time to look at those and get back to the committee with whether we have any views on those.

Senator LUDWIG—Thank you very much.

CHAIR—Okay. Thank you very much, Mr Pilgrim and Dr Clapin, and thank you very much for the submission from the Office of the Privacy Commissioner.

Mr Pilgrim—Thank you.

Proceedings suspended from 11.57 am to 1.34 pm

Williams, Professor George John, Private capacity

CHAIR—I welcome Professor George Williams, Director of the Gilbert and Tobin Centre of Public Law. Do you have any comments to make on the capacity in which you appear?

Prof. Williams—I appear in a private capacity.

CHAIR—The Gilbert and Tobin Centre of Public Law has lodged a submission with the committee which we have numbered 2. Do you need to make any amendments or alterations to that?

Prof. Williams—No.

CHAIR—Then we will go to an opening statement and have questions after that.

Prof. Williams—Thank you for the opportunity to make a submission to this process. I would like to start with an important caveat. The submission really focuses on B-party intercepts. I certainly lack expertise in this area and in a range of other matters that the committee might be dealing with. If I am asked questions, I am happy to have a go, but I cannot promise the answers will be correct.

My starting point when speaking about a law such as this is that we need to exercise great caution in dealing with a matter that the explanatory memorandum, the Blunn report and indeed a number of commentators have recognised as being one of great sensitivity. I am not suggesting that we can necessarily define a better word here but, when you combine low thresholds with difficult words such as 'security', we end up with a test that makes it surprisingly easy, I believe, to collect information from innocent parties, including information that arguably is not related to the core information that ought to be collected.

I think it is also quite significant that, if we look at paragraph 12.9 of the Blunn report, we see that it sets out a number of additional issues that ought to be in play when we are considering whether this information should be collected. It refers to information being clearly material to a relevant investigation or crime. That is not a threshold that is built into this legislation. It also includes the issue of the destruction of material that ought not to have been collected. Again, I do not believe that has been built in effectively.

The same problems apply, but in a different way, to section 46. The net there, again, is very broad, particularly in subparagraph (1)(d)(ii), even as modified by subsection 3, in that information may be collected under that. It is simply a matter of logically following through the provision, which may not actually assist with the investigation at hand. It is overbroad in terms of the scope of the legislation. The last point is that it strikes me as strange that there would be a double standard here between stored communications of the type we are dealing with and other forms of communications such as voice. Indeed, the thresholds and tests that apply to those different types of communications are different. It strikes me as nonsensical that a differentiation would be drawn between speaking to somebody on a mobile phone and sending them an SMS message. Many of the students whom I teach today see them as equivalent forms of communication. It makes no sense as a matter of law or public policy why, indeed, it is easier to gain one type of information than the other.

In conclusion, when I look at a law like this I start with the legislative purpose, and I think it has simply been poorly drafted. The checks and safeguards are not there, even with what I

think is the largely and admittedly low standard of the Blunn report on safeguards. It also says to me that this is the type of law that we can see, particularly in a system that lacks something like a human rights act or other charter of rights and responsibilities, that sets out legislative standards that ensure that rights like privacy are taken into account more directly and in a more concrete way so that we do not get legislation that simply misses some of the key issues that I believe ought to be included.

CHAIR—To take up your last point about the checks that are included in the Blunn report, in part 12 of the report—and it is really a very small part of the report, but a very significant step legislatively; the B-party interceptions aspect—Mr Blunn suggests some appropriate controls. He states:

> … a warrant must establish to the satisfaction of the issuing authority … to support their belief that the information likely to be obtained from the intercept is material to the investigation—

and so on. Those are the sorts of things which you think are important and ought to be contemplated in the legislative package we are dealing with?

Prof. Williams—Yes, and in particular those at 12.9. I acknowledge, as you said, that it is a small section for dealing with such a large issue, given the sort of precedent it creates. The one point I would perhaps fix upon more than others is the statement in the Blunn report that the intercept is material to the investigation. You cannot guarantee that that will be the case, as the legislation is currently drafted, because you could conceivably collect information that may relate to communications between second, third and fourth parties. Or you could simply have a situation where it is so broad that you end up collecting a large amount of information that may or may not be material. It is not built into the legislation, and that seems to me to be a crucial one to be included.

CHAIR—Just by the bye, Mr Blunn says at the end of 12.9, 'The use of such warrants should be separately reported to the parliament.' As I read the current legislation, the reporting is wrapped up with all the other reports; it is not separate reporting. Is that your understanding?

Prof. Williams—That is my understanding, and I do believe it should be separately reported. One of the problems is that the interception of innocent party information is caught up in exactly the same way as suspect party information. I think there are quite different issues involved. In terms of scrutiny of government, people ought to know when government is collecting this type or that type of information, because it is material and important.

CHAIR—Thank you. I will come back to other issues, if I have a chance.

Senator LUDWIG—The issue of B-party interception is obviously focusing a lot of people's attention. I do not know whether you have had an opportunity to look at the submissions of the Law Council or Electronic Frontiers. Although they object to B-party interception, both of those submissions go on to add: 'If the government is minded to progress the bill then here are some additional safeguards that should be included within it.' Are you of the more general view that the more safeguards the better to ensure that the legislation is not overwide, that it does not unduly trample on people's privacy rights and that there are protections in the bill to ensure that there is a balance struck between the ability of law enforcement agencies to effect their operations and the privacy rights of individuals?

Prof. Williams—I have read the Electronic Frontiers submission. I have not seen the submission of the Law Reform Commission. It may not have been available on your website yesterday when I downloaded them.

CHAIR—The Law Council's submission was received very late yesterday.

Prof. Williams—I have not read that, but I did read the Electronic Frontiers one carefully, if only to educate myself about some of these issues.

CHAIR—I did that too.

Prof. Williams—It did strike me that, yes, they do have some very sensible proposals about thresholds and narrowing the net and also ensuring that information, once collected, is appropriately used and that other information that ought not to be collected is not collected. For me, it is not a matter of simply the maximum number of safeguards; it is the right safeguards that are tightly focused. In fact, in many ways, I think it is better to have fewer but better safeguards because, if we end up with a very long list, it can perhaps focus the mind on the wrong areas, as opposed to the core problems relating to collecting only the right information only when it can be justified and any information that is collected where it does not fit into that is destroyed immediately.

Senator LUDWIG—A couple of submissions mention use and derivative use and also privilege. Do you have a view about those?

Prof. Williams—I do. My view is that, unless there are particular or special circumstances, privileged information, such as lawyer-client information, ought not be collected through this type of regime. There are good arguments whereby, if lawyers themselves were involved in activity that may be criminal or otherwise, that may well negate the privilege. I could accept that there may be reasons why it should be collected on that basis. Otherwise, the very nature of lawyer-client privilege is that, where the government itself tends to be the party on the other side of the litigation table, it is highly inappropriate that the government gets access to that very information. It casts into doubt the justice system in terms of how that information is used. It can lower public confidence and, except in those limited circumstances, I would prefer to see a clear exception for that type of information.

Senator LUDWIG—And use and derivative use? When you think about it in terms of the B-party, it is not only the B-party but also the C, D E and F parties who may at some point end up talking to B and, therefore, being captured. Does the concept of where you then say it should be destroyed form part of the original investigation or the purpose of the original warrant? Does that cover off on that issue, or should there be additional safeguards?

Prof. Williams—I am not sure that it does, though we are also coming to the limits of my own expertise in that this is a complicated area. Some of the technological issues are also complex in terms of who does fall within the net. My view is that it is better to be safe than sorry in an area like this, and it is very difficult through destruction only to be absolutely clear that the immunities you would expect to apply in such circumstances actually do apply. In the same way, it is common to see immunities, whether it be in the ASIO legislation or other bits of legislation, recognising that information can be collected inadvertently, otherwise it should not have been collected. I would prefer to see a clear, direct statement indicating that, if it does not fit within the information that could have been collected for a certain purpose,

immunities apply. I think it is inappropriate for enforcement agencies, simply through their luck or overboard legislation, to get access to information and then use it.

Senator STOTT DESPOJA—I want to start by asking you about the process queries and concerns that you have. Do you think this is an isolated circumstance or we are seeing a pattern developing with legislation of this severity, or arguably this controversial, being given minimal scrutiny?

Prof. Williams—I think there is no doubt that the level of scrutiny over the last nine months has been of a lesser quality than what we have seen before. Of course, it is not surprising that that is the case, but it has clearly been the case.

It does concern me because the sorts of laws that this committee, amongst others, has dealt with over the last nine months when considering the issues of preventative detention, control orders and other matters deal with some of the most significant legislative changes in the history of Australia. They are that important in how they deal with fundamental legal principles and have changed and realigned the relationship between the state and the citizen.

I am gravely concerned, I would have to say, particularly since the work that I have done overseas, in London and elsewhere, over the last couple of months demonstrates again and again that process is a necessary and key ingredient in getting the laws right. Without process, the odds are that laws are made too quickly without appropriate scrutiny. When we are dealing with novel and important issues like this, we end up with bad laws, as in the case of sedition. We simply have to investigate after they have been passed to determine whether it was got wrong in the first place. That is a mockery of process. I am not aware of such an instance—

CHAIR—We tried our best.

Prof. Williams—As I said earlier, I understand completely the sorts of views that have been put on this from a number of quarters but I am putting it on record in a way I have not done at any previous inquiry run by this or other committees because I think the dangers are obvious and of concern.

Senator STOTT DESPOJA—I can assure our chair that it is not meant as a reflection on the hardworking members of this committee. However, I am a little concerned when I hear witnesses, including the Office of the Privacy Commissioner today, suggesting that they are still grappling with the meaning, outcome or consequences of a schedule of the bill. It seems that some of us are grappling with it because there is an issue involving time. I would have thought there needed to be analysis of this not only in the current context but also in the backdrop you mentioned of charters of freedoms and rights. Because you brought that up, I am wondering if that suggests to you that we are looking in some way at the diminution of personal freedoms or rights—specifically privacy rights—in Australia when you look at legislation such as this and its potential impact and at the cumulative impact of comparable legislation.

Prof. Williams—I mentioned charters and rights in part because I feel as if I always have to mention these things before I come to the committee, and I think people would be disappointed if I did not mention them!

Senator STOTT DESPOJA—Indeed.

CHAIR—Profoundly.

Prof. Williams—When we are dealing with a law like this there is no doubt that it does limit privacy rights—no doubt whatsoever. The government is collecting information under this type of law that otherwise would be private information. It relates to people's behaviour and people's communications, and it is done in a way in which people may not even know that it is occurring. That is a clear breach of privacy rights. On the other hand, I am not someone who says that privacy rights should not be breached in appropriate circumstances. It is always about balance. As I have said on other laws, we need appropriate, well-crafted terrorism laws to deal with what I think is a significant threat to Australia. The problem is that it is incredibly difficult to work out where to draw the line, in part because we have so little time to think through an issue of such importance.

The other thing is that if this type of law was in the UK or elsewhere, it would be interpreted in light of a framework that says privacy is important, limited according to the public need. We lack that backstop, safeguard and framework. It means that with limited time we could end up with a law that is not going to have the same protections you would expect in any other democratic nation. I think that is also why many of our laws will have a different application to the laws we copied them from, such as from the United Kingdom. That could mean they are more detrimental to individual liberties than would be the case in the United Kingdom, even though the text in some cases is identical.

Senator STOTT DESPOJA—Thank you for that. On the issue of constitutional validity, you have referred to problems or potential problems involving federal magistrates and judges as issuing authorities. I am just wondering if you would like to elaborate on that for the committee. In fact, maybe you could give us your opinion as to whether or not you think the framework is constitutionally valid.

Prof. Williams—My view is that more likely than not it is valid. I raised it because it is often raised in the submissions we make as something the committee should be aware of. Whenever functions are conferred upon judicial officers or non-judicial officers, the committee clearly should be aware of the constitutional problems. I think we have the advantage here of the decision by the High Court on Grollo v Palmer in 1995 that held that judges in a personal capacity could make decisions about telephone intercepts and other matters. I think the most likely outcome is that that would be applied to uphold the legislation in this case.

On the other hand, as we say in our submission, this is a different scenario, particularly dealing with the nature of the information and the different set of thresholds. I raise it because there is enough scope that somebody may decide to challenge it. This is an uncertain area of High Court jurisprudence. It rests upon a couple of 4-3 decisions in some areas, and the court now is largely changed. It is also an additional reason for having a very strongly crafted series of safeguards and checks, because I think that the greater the clarity and the checks the more likely it is that it will not cause problems. If the High Court believes that it is a regime that is somewhat at large or arbitrary, that is exactly the sort of thing that it is likely to say will bring

into disrepute those judges involved. It gives a reason to get the legislation right—to avoid those constitutional hassles.

Senator STOTT DESPOJA—Thank you. I will not ask you about the frameworks, the safeguards or the quarantine provisions to which you referred because I think my colleagues have done that. What is your understanding of the rationale behind that different treatment of communications? You referred to the differential treatment and the fact that many of your students, for example, would not quite understand why stored communications were dealt with in a different or specific way. I am wondering if you understand why the government has approached it from that perspective.

Prof. Williams—No. I have looked through the information, though, again, time limitations may well mean I have missed something on this. I had a student also search this issue to see if they could find what we might see as a sufficient or rational justification. I could not find one, and then I sought to develop one, I suppose, to see what might be the rationale. Again, it does not make any sense to me, particularly if you start from the starting point that, in the end, this is about privacy. I think the proper focus for assessing this legislation is: what is the appropriate limitation upon the privacy of Australian people? For them there is no rational distinction, so I cannot see how you could justify one from the government's end. They are the ones imposing the intrusion. They ought to live with the privacy rights and modify them only as necessary.

Senator STOTT DESPOJA—I have no doubt we will hear from the department on that rationale. Thank you.

Senator LUDWIG—I think it was EFA's submission, though I am happy to be corrected, that indicated a concern about magistrates issuing these types of warrants, particularly the stored communication warrant. However, your submission is that it would be more likely that a magistrate could do that, or would you say it applies equally to judges and magistrates?

Prof. Williams—The principle would apply equally to all federal judges, which includes the High Court, Federal Court, Family Court and Federal Magistrates Court. It would not make any difference. All of them are considered federal judicial officers and are subject to the same protections under the Constitution.

CHAIR—Thank you very much and thank you also for your submission. The committee finds it very helpful.

[2.02 pm]

GIFFORD, Mr Cameron, Acting Principal Legal Officer, Security Law Branch, Attorney-General's Department

HUME, Ms Maree, Acting Senior Legal Officer, Security Law Branch, Attorney-General's Department

McDONALD Mr Geoffrey, Assistant Secretary, Security Law Branch, Attorney-General's Department

COLVIN, Federal Agent Andrew, Chief of Staff, Australian Federal Police

LAWLER, Federal Agent John, Deputy Commissioner, Australian Federal Police

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

CHAIR—Welcome. I ask each of the agencies to address their submissions separately, where we have submissions, and then we will go to questions. I remind senators that under the Senate procedures for the protection of witnesses, departmental representatives should not be asked for opinions on matters of policy and, if necessary, must be given the opportunity to refer those matters to the appropriate minister. Do the Australian Federal Police wish to make an opening statement?

Federal Agent Lawler—I will make a very short opening statement. The AFP welcomes the committee's invitation to appear before this inquiry into the Telecommunications (Interception) Amendment Bill 2006. The AFP supports the proposals in the bill to address lawful access to stored communications, to clarify the legal basis of B-party interception, to authorise the interception of telecommunications services on the basis of a device, to remove the distinction between class 1 and class 2 offences for the purposes of applying for telecommunications interception and to replace the telecommunications interception remote authority function that the AFP currently performs with a warrant register to be administered by the Attorney-General's Department.

The AFP believes that one of the bill's strengths is that its proposed provisions will clarify areas of complexity and ambiguity in relation to accessing stored communications, particularly for law enforcement officers on the front line. The bill will make it clear to these officers what they can and cannot do. To that end, the AFP has worked closely with the Attorney-General's Department to ensure that its operational concerns are addressed as far as is possible within the regulatory framework established by the Telecommunications (Interception) Act 1979. The AFP has done this in an environment of constricted time frames and competing legislative priorities which have been impacting upon it. The focus of our dialogue with the department has been on the proposed regime for accessing stored communications, particularly via existing lawful means, and the proposed stored communications warrants. This dialogue is ongoing to ensure that the intent in the bill to distinguish between overt and covert access of stored communications does not undermine the way the AFP currently accesses stored communications, by overtly using search warrants, arrest powers or other lawful means.

As the committee is aware from the submissions it has received, some agencies have expressed concerns about the introduction of the stored communications warrant as the lawful

means to access stored communications covertly from carriers and internet service providers. To an extent, these views reflect the AFP's position on stored communications. The government is aware that the AFP still believes that the application for search warrants under the Crimes Act 1914 is an appropriate authorising process for accessing stored communications. The AFP understands that the proposal in the bill for stored communications warrants is focused in particular on access to stored communications without recourse to an issuing authority in the case of those police forces, particularly with standing warrants, or those regulatory agencies that issue administrative notices.

The AFP believes that accessing stored communications from carriers and internet service providers without the knowledge of the recipient is likely to be an increasingly important investigative tool in the future. Therefore, the AFP will be monitoring its use of the proposed stored communications warrant regime to identify any issues that may undermine its operational effectiveness in order to bring those forward to the government for consideration. Thank you for the opportunity to make this opening statement.

Mr McDonald—This bill amends the Telecommunications (Interception) Act to implement the recommendations of the *Report of the review of the regulation of access to communications*, which is called the Blunn report. The review examined the issue of how best to regulate access to communications in the ever-changing world of telecommunications technology. The Blunn report concluded that the ability of law enforcement and security agencies to use telecommunications interception and other communications data to identify organised crime networks is an invaluable tool in the fight against serious crime and terrorism. This is all about keeping us up to date with developments in technology and enabling them to do their job. The report also concluded that the act required amendment to maintain an appropriate balance between privacy protections and meeting the needs of security law enforcement agencies. That is what we have been attempting to do.

The bill is the first step in implementing the recommendations of the Blunn report to create overarching legislation to ensure that the interception regime accommodates new and emerging technologies. The government is continuing to consider all other recommendations outlined in the Blunn report such as the proposed review of aspects of the Telecommunications Act. The recommendations that are implemented in this bill, though, need to be put in place because of the imminent expiry of the sunset clause and because of real operational needs. Police have been concerned about the operational problems in this area for some time and have shown some patience as we have tried to deal with these issues.

As with many legislative packages, there are submissions that bemoan the speed at which the bill has developed and that suggest that it is overly complex. We have also had others that have said that it has taken too long and they would like to make the bill more complex. The bill is fairly long, and I just want to explain that some of that is to do with the structure of it, the consequential amendments and the like. That means that the bill itself is no Mills & Boon to read, but we have been aiming to ensure that the Telecommunications (Interception) Act itself is in fact easier to use. The little summary which I think I gave to the committee gives you a bit of an idea of what the chapters will end up looking like. I guess the approach we have always taken here is to try to separate the relevant procedures in a way whereby the

police and others using the legislation can go through the steps. That is why it is drafted in the way that it is.

I should add that why I refer to the word 'patience' with respect to the issues of getting the relevant powers and the like is that the Blunn review started almost a year ago and we have a situation where the police are trying to deal with the operational needs that they are confronting on a daily basis. I point out that when Blunn started his review he had public consultation. In the back of his review, you will notice that there are comments from many organisations that were represented before this committee today—the Privacy Foundation, Electronic Frontiers, ASIC, SingTel—but not from the Law Council of Australia. This was advertised in the papers and these other organisations were able to get involved and become engaged in it, yet we hear that this is the first time the Law Council has heard of it.

I just point out that, contrary to what was said by the Law Council and what was just said by George Williams, we have had a consultation process with this and we do try to consult on our legislation. There are situations—like with the terrorism bill last year where there were real concerns about getting the legislation in place before the holiday period and, of course, the Commonwealth Games—where we have to do things in a more accelerated manner. But there is as strong a commitment from our department and from the government in terms of consultation as you will find in any other country, particularly the United Kingdom.

I should mention that we have been dealing with converging technologies—which is what a lot of this is about—going back to the Cybercrime Act of about five years ago and leading up to telecommunications offences of recent times. This is just another example of our efforts to keep up to date with the fact that new technology is used to commit crime and to avoid detection. I look forward to answering your questions.

CHAIR—Thank you very much, Mr McDonald and, again, thank you, Deputy Commissioner. Thank you all for appearing today. Mr McDonald and his colleagues have had the extraordinary benefit of spending the whole day with us, so they are truly blessed!

Mr McDonald—Absolutely.

CHAIR—I will suggest to my colleagues that, by and large, we try and move logically through the bill. Or perhaps not?

Senator LUDWIG—We can try!

CHAIR—I would do that with one glaring exception, which I regard as the chair's privilege. But first, let me just check something with you, Mr McDonald. We have a submission, which I think we received today, from the Australian Communications and Media Authority. It is about a concern they have about the effect of this act on the Spam Act and their capacity to access what are defined in the Spam Act as unsolicited commercial electronic messages. They indicate in the submission that the issues raised can be remedied through minor amendments to the bill and that they are working with the AGD to develop a proposal for such amendments that would exempt investigations under the Spam Act from the stored communications warrant regime. What is the department's view on this matter?

Mr Gifford—This is an issue that ACMA has raised with us previously. It is a matter on which we continue to work collaboratively with ACMA and the Attorney is well versed in this

particular issue. To the extent that ACMA has foreshadowed that an amendment might be necessary, it is out of our control to actually foreshadow any amendments that might be necessary to achieve their given outcome, but we are progressing this matter with ACMA.

CHAIR—So if I were to send this to you for formal response as a question on notice, is that what you would say to me?

Mr Gifford—Yes.

Mr McDonald—We have governmental processes that seem to continue beyond when bills get introduced, on occasions, and as soon as we are in a position to provide something further on that, we will. We expect that it will be resolved pretty quickly.

CHAIR—The committee might raise this question with some of our other witnesses today, to have a look at their response on the issues ACMA raise. I can see Ms Graham looking interested!

Senator LUDWIG—I am trying to understand the difference between a sent email and one that is returned because it did not get to the intended recipient and is then stored in the sent box. It never got to the intended recipient, although it did get to the ISP. Is that a stored communication?

Mr McDonald—Yes, well, it is—

Mr Gifford—Under the current definition proposed in the bill, that would not be a stored communication to the extent that it would not be accessible to the intended recipient, that being the email addressee who was intended to receive it had it not been bounced. To the extent that we continue to examine the provisions of this bill, we have been made aware that this might cause some problems for our agencies in that it would remain subject to the telecommunications interception regime. So we are still working with our agencies to make sure that there are no unintended consequences from that particular provision in terms of the new proposed definition of passing over the telecommunications system. But so far as the bill is concerned, it will still be passing over and subject to TI.

Senator LUDWIG—The difficulty that will then come in is that you will have to look at the inbox to know that it is a sent item that has been returned because, if you access the ISP, the ISP will still have it in there as an unsent item.

Mr Gifford—That issue has been raised more broadly in that the way we are defining 'stored communication' and 'passage' is by reference to something that is accessible by the intended recipient. That question, of whether or not access is available via the sender, is still under active consideration by the government in terms of making sure it makes sufficient allowance for our operational needs.

Senator LUDWIG—What about the sent box itself?

Mr Gifford—To the extent that our communication has passed over and is accessible to the intended recipient, it becomes a stored communication and would not therefore be subject to telecommunications interception.

Senator LUDWIG—It would be the 3L that enabled it to be accessed?

Mr Gifford—Depending on the means of access. I think that is a point we have to make very early with stored communications. What we are setting up here is a regime that has two points of access. The first point of access is via carriage service provider without the knowledge of the intended recipient. In that instance a stored communications warrant will be required.

Senator LUDWIG—That is a covert.

Mr Gifford—That is a covert. If you are accessing it overtly with an existing general search warrant power, such as 3L of the Crimes Act, you will be able to get access to those communications. We have not altered the position of 3L.

Senator LUDWIG—Where do instant messages sit?

Mr Gifford—Quite strangely, is the short answer. If you ever get instant messaging at the point where it is still in its passage it will be subject to telecommunications interception, but you would have to be moving very, very quickly. Where you are accessing it with the knowledge of the intended recipient, it becomes a stored communication. Again, that broader question of access via the sender remains to be resolved.

Senator LUDWIG—Instant messaging may involve 15 people. Is it the knowledge of all of those 15, or just the knowledge of one?

Mr Gifford—Knowledge of the intended recipient from which you seek access.

Senator LUDWIG—But you could be sending it to 15 people. If it is a messaging service—and forgive me if I am getting this wrong—you could send the text message to all of those people that might be online at that particular time and who can access your site. You have allowed them to be able to communicate with you. They might be logged on or logged off. You will have an icon—perhaps I am displaying too much knowledge—that will indicate whether they are online and can receive your message. Do all of those people have to know?

Mr Gifford—There is no requirement in the bill that every party to that communication would have to be notified of the access.

Senator LUDWIG—Where does it fit in the scenario where someone is sending a short message to four, five or six others, for example?

Mr Gifford—If you were sending a short message to every person at this table and one of our agencies was to seek access as I receive it, and they give me the knowledge that that is going to be accessed in that manner, that can be accessed as a stored communication.

Senator LUDWIG—We have covered short messaging. What if you have to use a password to access the computer to press send and receive? Depending on the style of email service you are using, some will bring it automatically into your email box; some will require a person to press a send button. If the AFP exercise a warrant under 3L, they go to the computer or their mobile handset and press send to receive the information, should they have then obtained a stored communications warrant, a TI warrant, or can they use 3L to press the button?

Ms Hume—Our intention is that, if they have the power under 3L to use—I understand the legislation is worded 'reasonable'—

Senator LUDWIG—Let us take as an example a person who stands idly by. You can get anything you like, I suspect, by cooperation.

Ms Hume—If that is allowed under the current provisions of 3L then that is what would be allowed. This regime is not changing the operation or the scope of 3L.

Federal Agent Lawler—That is a very important point that you raise—for law enforcement officers at the front line to have certainty and no ambiguity. An example might be a drug courier coming into Australia who is taken into lawful custody and the drugs located. That person has a mobile phone that might even be receiving messages as you are speaking, possibly from somebody waiting outside in the main arrivals hall. An SMS message quite clearly is accessible if the person is in lawful custody. There is power to search and to seize items on their person. Also, there is the need—as you are saying—with the 101 type scenarios for officers to be able to access that material. It is my understanding that that area is certainly captured in the legislation.

Mr McDonald—Section 3L(2) says:

(2) If the executing officer or a constable assisting, after operating the equipment, finds that evidential material is accessible by doing so, he or she may:

… … …

(b) if the material can, by using facilities at the premises, be put in documentary form—operate the facilities to put the material in that form and seize the documents so produced.

Senator LUDWIG—101 is voice, so is that captured by 3L? It is not documentary. There are many different types.

Ms Hume—The policy intent of the legislation is in the way we have defined 'accessible to its intended recipient', which is received by, delivered to or in the control of 'the telecommunications service' of the intended recipient or of 'the intended recipient'. Under the current search warrant powers or Crimes Act powers or other enforcement powers of law enforcement agencies throughout the states and territories, including the AFP and other Commonwealth agencies, agencies currently have the power to access those communications via the intended recipient. If it is defined as being that the communication ceases its passage once it is accessible—that is, received by, delivered to or in the control of the intended recipient—then it falls outside the interception regime. Say that communication is held by a carrier. Our policy intention is that, where a law enforcement agency goes directly to the carrier without the knowledge of the intended recipient to access the communication, that is where the stored communications warrant regime kicks in. If they are going to the intended recipient or to the premises where they are exercising their lawful existing powers—for example, under a 3L or another Crimes Act warrant—then that is where those powers fall outside our regime. Does that clarify it?

Senator LUDWIG—I understand the policy intent. I think I understand passing over and I understand what you mean by the definition. What I am trying to establish is that there is not a grey line. In fact, there may be a black line. Quite frankly, the law enforcement agencies know exactly what they can and cannot do in most circumstances. There is always going to be a circumstance where they might pause. In this instance there needs to be at least clarity, because you do have actions that can be defined.

Mr McDonald—I have heard what the deputy commissioner has said. We will certainly be making absolutely sure that there is clarity about this. It is something that we will reflect on further. We will get a mark 2 back fairly quickly.

Senator LUDWIG—Chair, it is really a case of how you want to deal with some of these matters. The EFA raised a range of issues which are quite relevant, quite frankly, in terms of trying to clarify how the stored communications regime works. At 3.1.1 of their submission they say:

The ... definitions leave open to question whether or not a copy of a communication ... is also a "communication" ...

They also say at 3.1.2:

EFA considers the definition of record should be amended so that it applies in relation to, not only an interception, but also accessing a stored communication.

They also talk about matters to do with a person, which is also a relevant issue, at 3.2, 'Stored communications warrants'. Do you want to go through each of those individually, although that may take some time, or if I tag them can we ask the Attorney-General's Department to come back with an explanation at some point? If the Attorney-General's Department feel sufficiently minded, they could provide an explanation today.

CHAIR—I would be keen to get as much on the record as we can as a result of today's hearing. Apart from anything else, as the department and everybody else is acutely aware, we have a very tight turnaround.

Senator LUDWIG—I was worried about the time it might take.

CHAIR—And we also have another pending legislative report on another bill, which needs to be finalised in that same time frame. I think we can deal with most of the detail that has been raised with us. Some of it is in stored communications; I think the bulk of it is in B-party intercepts, which we are keen to explore with everyone. The questions are relatively easy. I am not sure that it will take that long. For example, does a copy of a stored communication require a stored communications warrant to be accessed, or does it only require a search warrant? What does the bill actually mean in that regard?

Mr Gifford—A copy of a stored communication accessed by the person on the premises—so any end point of the communication—will not require a stored communications warrant. It is only those communications which are accessed directly from the carrier which will require a stored communications warrant. Existing search warrant powers in terms of 3L and the like will get access to a copy of the communication—or, indeed, a warrant will be required to access with the knowledge of the intended recipient.

Senator LUDWIG—And the definition of communication is reflected in the definition of stored communication?

Mr Gifford—Yes. To be a stored communication, it must first be a communication, so it picks up on that definition that exists in the interception act in terms of being a record of a message.

CHAIR—Mr Gifford, I think you have been to the Attorney-General's Department witness training school which requires people to speak at a rate that the human ear actually cannot

hear. One of the advisers in the Attorney's office graduated with honours from that school, but it would be much easier for us all, including the other witnesses, if we could hear and understand what you are saying. Could you please slow down?

Mr Gifford—Not a problem. I certainly shall.

CHAIR—Thank you very much—and you might want to repeat what you just said to me!

Mr Gifford—In accessing a communication at either of the end points of the communication—at the end user—you will not require a stored communications warrant unless you choose to get access to that overtly via the carriage service provider. In terms of Senator Ludwig's question, a stored communication must fit within the definition of communication before it can also be a stored communication.

Mr McDonald—Earlier testimony commented on that, and we agree.

Senator LUDWIG—At point 20 on page 8, it says:

20. Both the above definitions refer to "recording" a communication which is defined in the existing Act as follows:

And it provides a definition. Then it goes on:

21. EFA considers the definition of record should be amended so that it applies in relation to, not only an interception, but also accessing a stored communication.

Mr Gifford—This is the first time I have had a chance to have a look at this particular part of the EFA submission. It is certainly something that we are more than open to considering.

Senator LUDWIG—It does look like there is a gap there. On stored communication 3.2, page 9, why do you say 'in respect of a person' where I think the explanatory memorandum says stored communications warrants are more similar to named person interception warrants and to telecommunications service interception warrants?

Ms Hume—A stored communications warrant can be served on the carrier under the new regime where the person is listed. For example, if I were under investigation, the police force could issue a warrant to the carrier with my name on the warrant, and they could pick up the stored communications. I may have an email account, a mobile phone and other forms of stored communications. Under that warrant, they would be able to have access to my stored communications held at the carrier.

Senator LUDWIG—Is the stored communications warrant able to have the name of the person and details sufficient to identify the communications services in relation to which access is sought?

Ms Hume—The warrant would include the name of the person whom the warrant is over, including the telecommunications services that the stored communications would be attached to. All the other relevant details would be included in the affidavit. The facts and the grounds for issuing or applying for the stored communications warrant are required to be included in the affidavit.

Federal Agent Lawler—That is not to say that those details are necessarily true details.

Senator LUDWIG—Further, it goes on to indicate that there does not seem to be a requirement to provide information about previous stored communications warrants. Would that be done as a matter of course?

Mr McDonald—There would be plenty of situations where that would be a relevant circumstance.

Mr Gifford—One of the limitations on the access to stored communications warrants is that you can only get a warrant every three days in relation to a particular service used by a person. So with any application the issuing authority must have regard to whether or not you are inside that three-day time frame and, if you are not inside that time frame, whether or not there have been previous applications for stored communications warrants.

Senator LUDWIG—So would you have to say that you are accessing it for the fourth time, three days in a row?

Mr Gifford—There is nothing expressed in the bill at the moment that requires that. I must admit that the department is currently working on the prescribed forms for which the stored communications warrants will be made.

Senator LUDWIG—It would seem a sensible thing to tell the issuing authority that this is the fourth time for the third day. You would leave yourself open—

Mr McDonald—The police would agree with me that you would be really opening yourself up to major problems with the courts if you did not reveal such information. But, certainly, in the forms that we will be putting together in this area we will be guarding against misunderstandings of that nature. I think that will be in the interests of all of us who are involved. The police would have exactly the same view. I should not speak on your behalf, but I think you would agree.

CHAIR—The deputy commissioner will jump in if he disagrees.

Mr McDonald—I know!

Federal Agent Lawler—On that point, it is our normal practice to make such notifications to the issuing authority. That happens across a range of warrant applications. That having been said, in a practical context I would think it highly unlikely for there to be a need to go back on a regular basis, such as you have outlined. More likely what would happen would be that, if it were still relevant and necessary, we would be moving towards a full telephone intercept of the service concerned. I understand from other submissions that there has been an issue with the three-day period and, in extremis, what might happen if in fact you needed to access stored communications within that period. The act is quite definitive there. That is of course an issue, but my sense, and my judgment, is that if it was in extremis and of such moment there would be other opportunities open to us to access that information through the Telecommunications (Interception) Act.

Mr McDonald—If you look at the things that have to be considered when these are being issued, you see that the matters that the issuing authority has to take into account include a person's privacy and how the warrant fits in with the investigation. There are a whole heap of things there that the issuing authority must have regard to. That is in section 116(2). So if the

details to be provided to the issuing authority did not have something of that nature in there I think there could be some real difficulties.

Senator LUDWIG—The other area is the penalty regime. EFA make the point at 73 of their submission:

> As the threshold for issuing stored communications warrants is itself 3 years imprisonment or 180 (900) penalty units, we question the justification for allowing accessed information to be used in relation to offences and civil contraventions involving lower penalties than the warrant issuing threshold.

They then rely on the Surveillance Devices Act 2004, which:

> ... enables warrants to be issued in relation to offences punishable by a maximum term of imprisonment of 3 years—

and others—

> but does not permit any information obtained from the use of a warrant to be used in relation to offences involving lower penalties than the warrant issuing threshold.

It would seem sensible, given EFA's submission—

Mr McDonald—It is interesting. It is more consistent, though, with the regime we have with search warrants, where there is not less—

Senator LUDWIG—Do not tell me any charge will do. I am sure that is not the AFP's view.

Ms Hume—I may be able to help in relation to this. Surveillance device warrants are for 90 days ongoing. So if a surveillance device is installed the warrant is for 90 days ongoing access to the information retrieved from that surveillance device. Under the stored communications regime it is a historical snapshot; it is not ongoing access. It is analogous to a general search warrant, which, if you go to the carrier and exercise a stored communications warrant, gives you those stored communications which are currently in existence.

We have designed our regime so it does not undermine the telecommunications regime. That is why we have said that a stored communications warrant cannot be issued over that same telecommunications service for a further three days, so that there are not rolling stored communications warrants, which would mean telecommunications interception at a lower threshold.

The way the telecommunications interception regime works with use and disclosure presently is that generally a seven-year offence is required to be issued with a telecommunications interception warrant. The period of use of that telecommunications interception material obtained through that warrant can be dropped to as low as three years, or the material can be used for a permitted purpose as provided for in the act, which has a lower threshold than you would need originally to have the warrant. Our regime has been designed to mirror that in the sense that you have the initial threshold of three years or 180 penalty units. The penalty for the use of that is then dropped to one year's imprisonment or 60 penalty units. So the initial privacy intrusion is at a high threshold. The use of that is further allowed for—

Mr McDonald—If you come across something.

Ms Hume—if you come across something during the investigation of an offence which does carry a three-year prison penalty.

Mr McDonald—It reflects the policy of the TI Act.

Ms Hume—In the Surveillance Devices Act it is 90 days ongoing and therefore the threshold is maintained for at three years across the board.

Senator LUDWIG—Does that include civil penalties?

Ms Hume—If I understand the question correctly, you are asking if there is a lower threshold for civil penalties?

Senator LUDWIG—Yes.

Ms Hume—It is 60 penalty units.

Senator LUDWIG—It is based on a penalty unit, so it is not only criminal; it is also civil.

Ms Hume—That is correct.

Senator LUDWIG—What is the rationale for that?

Mr Gifford—It is part of the policy balance that we have tried to strike between the privacy protection and the level of access that is currently allowed by the stored communications provisions that were put in in 2004. Those provisions essentially made an exception to the general prohibition against interception subject to any general lawful access. As we have heard today, those general lawful access provisions have been read down to say, 'If I have a notice to produce then I can use this information in any way I see fit.' We are lifting that threshold to three years and then use for one year. At the same time as saying that we are lifting that threshold, we still have to recognise that for the past 12 months all of the regulatory agencies have had a greater degree of access. As ASIC testified this morning, this would have a significant impact in terms of their use of this power if it was to be any higher.

Senator LUDWIG—That is not a justification, though, with respect.

CHAIR—That is not a matter Mr Gifford can comment on. The committee can, though, and will.

Senator STOTT DESPOJA—I was curious in relation to the criticisms you have heard today and the concerns that have been raised most recently by Professor Williams about the extension of issuing authorities in relation to stored communications warrants. I am wondering if the rationale for that is simply that it is easier than for a telecommunications interception warrant. Also, how is your legal advice looking? Professor Williams seemed pretty much on side, in a legal sense anyway. I do not think it was about to be declared unconstitutional. Perhaps you can give me the rationale and tell me how you respond to the concerns that have been raised by a number of witnesses.

Mr McDonald—The first thing is that we have conferred with our chief general counsel, so we are confident about the legal aspects to it. It is good to see Professor Williams agreeing with us. In terms of using the range of issuing authorities, what we are doing here is, as I said at the beginning, trying to get a balance. ASIC said earlier, 'We don't see why these electronic things should be treated any different to any other hard copy document.' So you have that angle to it. Of course, a search warrant can be issued by a magistrate, and of course we have

discussed section 3L, which talks about circumstances where you can get stuff that is already on the computer. I think Tony Blunn in his report makes this point that there is a distinction between something that is live and something that is being composed and stored like a document. Consequently, because of those factors, Mr Blunn recommended that it was appropriate to have it as a magistrate. There are obviously logistical issues that come into it, and I guess some of the same logistical issues that lead us to wanting to use a magistrate for a search warrant come into it as well. However, in our view the stored communication is different to a hard copy document, but it is also different to something that is going live across the network.

Senator STOTT DESPOJA—Can I pursue that. First of all, I acknowledge the Blunn report in relation to recommending a maintenance of the distinction between real-time access and stored communication. But I want to get to the rationale when you talk about that distinction. Is it on the basis of technical or technological difference, or is there also this implicit assumption that one is more private than the other—one is more considered than the other? I am wondering, based again on the brief comments by Professor Williams and his reference to his students, who may have a certain opinion: is it not fair enough in this day and age that we do treat those communication forms similarly?

Mr McDonald—I had some quite interesting discussions with Mr Blunn about this issue, and it is not an easy one, but certainly the idea that it is slightly more considered is something that was in his mind or was something that we discussed. It is something that is in writing—something that definitely involves more consideration of the expression—although there is the speed issue. Some people can send text messages quite quickly compared to me; it is quite impressive.

Senator STOTT DESPOJA—I think the chair and I are both looking guilty at this point in time.

Mr McDonald—My messages are usually in very long sentences rather than the more abbreviated form, I can assure you.

CHAIR—It is called SMS for a reason.

Senator STOTT DESPOJA—I think it is quite a fascinating question, given that I would love to think that I put much more effort into an email than I would a phone conversation. However, these days I am not so convinced. That is not a reflection on my emails—

Mr McDonald—You certainly do in the Public Service, because a badly thought through email could cause problems. I think there is a motto: 'Emails should be twice as gracious and polite as you would be in person, because the written word can be taken very badly.'

Senator STOTT DESPOJA—I think it is still a matter of debate, but obviously my original question related not so much to the differential treatment in terms of definitions but to the issuing warrants.

Mr McDonald—We have heard people arguing for the thresholds to go in either direction. Certainly Mr Blunn consulted a lot of people, as we heard from the Office of the Privacy Commissioner. I think it was a fairly warm compliment about the way he engaged in his

consultation. I know from conversations I had with him that he gave this very careful consideration.

Senator STOTT DESPOJA—Because the reference to ASIC has been made, I am wondering if you have a specific response to some of—

Senator LUDWIG—I am going to ask about that, but before I go there I want to hear from you, Mr McDonald, about the issue that Mr Gifford raised earlier. The difficulty for me is that it would have coloured my view back then as it is now if you were going to rely on the fact that this committee recommended a relaxation for a period to allow a review as an excuse to then say, 'We've allowed it for 12 months and therefore it should now be relaxed, because people have used it.' If that was the case that was put to me 12 months ago—it would be longer now—I would have opposed strenuously allowing a review with a relaxation. I suspect the AFP would have been disappointed about that. I may not have got my view up, but I certainly would have progressed it.

Mr McDonald—All I can say is that there has been a very genuine and careful review used during that period. I think the review period was extended for several months, for six months.

Senator LUDWIG—And we agreed to that.

Mr McDonald—Yes, you agreed to that so that it could be done.

Senator LUDWIG—For the right reasons.

Mr McDonald—Yes. All I can say is that a genuine effort has been made, as far as I can see, by Mr Blunn and our department to come—

Senator LUDWIG—No, you misinterpret me. I understand that the review was a good review, and every effort was made by the department to ensure that there was an independent review and that it was thorough. That was also the basis for the extension, that we would ensure the department did have sufficient time to read the review and come up with an outcome, and therefore the extension of the current regime as it was then, we found out, 3L rather than a telecommunications interception regime. That led to a position where there was a significant relaxation, at least from our perspective of what we thought the law was, when in fact the AFP advised us it was otherwise. We then accepted that as a status quo, but only as a status quo, not to be relied on to then say, 'Given that you've allowed a status quo for 12 months or more, that is reason enough to allow a relaxation to continue.' If you had told us that back then, that you were going to use that period for that purpose, I would have opposed you.

Mr McDonald—It is certainly not the position anyone here would have seen as what was to be coming out of it. I was not in this position at the time this was quite an issue, but I think everyone appreciated it was designed to give a little bit of breathing space. From what I could work out it was a really genuine misunderstanding, and what has been done is that parliament has sensibly given sufficient time for there to be a proper review. I do not think anyone—certainly not in our portfolio—is suggesting that the fact that that was agreed to for that period is reason in itself for relaxing it.

Senator LUDWIG—They are the words I needed to hear. We can move on, thank you, unless AFP wants to add something.

Federal Agent Lawler—Yes, I would. I was fortunate enough to be here on the occasion when the bill was debated before this committee. From an AFP perspective, there was ambiguity and lack of clarity around what was the lawful position. Certainly the position of the AFP up until that time had been to access the communications. We believed we were doing so lawfully and that it was appropriate, and there was advice to that effect. What happened with the committee's deliberation and the subsequent passage of that bill is that it supported that position while the review took place. So it was the status quo and, in our view, appropriately so.

Senator LUDWIG—Notices to produce: we have heard from ASIC and they put an interesting position. There is also an EFA position which says that section 280 of the telecommunications legislation might in fact cause ASIC some difficulty in what they are currently doing. Do you have a view about that, representing the first law officer?

Mr McDonald—That particular provision will be something that we will take ASIC through when we have an opportunity to talk to them. We do not administer that provision—it is the communications department—so I would not really want to be expressing a view on it. However, the position is that —

CHAIR—Ask it the other way around.

Senator LUDWIG—Is a notice to produce permissible to the extent that ASIC have been using it under the current regime?

Ms Hume—My understanding is that they have very broad powers under their act and their notice to produce refers to documents, including documents held in electronic form. From the evidence ASIC provided this morning, they were giving the example of where an email attachment is sent. It is perhaps a very broad definition under their act which allows them to use their notice to produce. Whether that legislation is inconsistent with the telecommunications access regime under the Telecommunications Act is a matter between those departments, from my understanding. We do not administer that legislation.

Mr McDonald—One thing is for sure: this bill will clarify what the position will be with stored communications. As you have heard from ASIC, they are not totally enamoured of every aspect of it.

Senator LUDWIG—I think 'happy' is the word.

CHAIR—Do you say it will clarify, Mr McDonald, the capacity that they have ably demonstrated to get around it using other provisions? Are you suggesting that will no longer exist?

Mr McDonald—That is right. We will have ongoing discussions with them on this.

Senator STOTT DESPOJA—On the ASIC evidence, not directly related to that question: I note there was reference to pecuniary penalties or something that they said was based on the states and they were sure it was an inadvertent, presumably, drafting issue. Are you able to elaborate on that for us? Was there something inadvertently not put in or not updated in the bill?

Ms Hume—The proposed section 5E, which defines a serious contravention when a stored communications warrant can be applied for and issued, specifically refers to 180 penalty units. In subsection (3) of the provision it says:

To avoid doubt, a reference in this section to a number of penalty units in relation to a contravention of a law of a State or a Territory includes a reference to an amount of a fine or pecuniary penalty that is equivalent, under section 4AA of the Crimes Act 1914, to that number of penalty units.

It is my understanding that 4AA of the Crimes Act already allows that interpretation of the monetary value of penalty units at the Commonwealth level. It is for the avoidance of doubt that section 5E(3) is included, so that state and territory legislation is also covered, but 4AA of the Crimes Act allows for that already.

Senator STOTT DESPOJA—It is just added clarification, by the sounds of things.

Senator LUDWIG—Section 4AA has a way you calculate it out.

Ms Hume—It is the way that it is calculated. That defines it at the Commonwealth level, and that is why we have put a for avoidance of doubt provision only for state or territory. ASIC may have been misinterpreting our intention in subsection (3).

Mr McDonald—We will have ongoing discussions with them.

Senator STOTT DESPOJA—I bet you will. I mean that in a positive way.

CHAIR—Before we move to the issue of B party, I have some questions about the issues the Office of the Privacy Commissioner have raised about material that is collected. Their submission notes—I do not now if you have had the chance to look at it—that, given the breadth of material that will be able to be collected by a number of agencies under these proposals, we may end up with a lot of material that is not relevant to the specific inquiry at hand. They are concerned about a more rigorous process of managing that and disposing of it appropriately within an expeditious period of time, not when someone gets around to it. What are your comments on their observations about that management process?

Mr Gifford—Section 150 of the bill provides that there must be destruction of the material once there is no longer a purpose connected with the investigation of the offence in relation to the agency. The comments, as I understand them, from the OFPC suggest that there might be a way to evade a time lag should the chief officer of the agency not turn his mind to it in an expeditious manner. If that is the case—and I would not expect that would be the case with any of our agencies—there is a general prohibition—

CHAIR—Not just your agencies, Mr Gifford. Bear in mind the breadth of agencies that are going to be able to use these mechanisms.

Mr Gifford—This is true. There is also the additional safeguard that there is a prohibition on the use of any information. So to the extent that there is not a use connected with the investigation, they cannot use that material right up until the period it is destroyed.

Senator LUDWIG—The Privacy Commissioner is referring to a disconnect between 'forthwith' and 'is satisfied'. If you tie that together with a forthwith as well for the consideration, you are required to forthwith destroy—but only once, effectively, the chief officer turns his mind to it. If you are a reasonably big agency you might not want to turn your mind to it.

CHAIR—I understand that there is a reporting requirement, but it is not apparent on that face of the legislation that, Mr McDonald, 'they will have procedures'. This is important, given the breadth of agencies we are talking about now. We are not just talking about law enforcement agencies or agencies that are used to dealing in these matters as a matter of course; we are talking about agencies like ASIC and others. So the committee would be grateful for the department turning its mind to that issue just for starters.

Mr McDonald—Okay.

Senator STOTT DESPOJA—While I acknowledge that there is a prohibition on use of that information, for some people—say, privacy advocates—the issue is not simply whether or not the information is used in another manner or destroyed but the fact of someone having that information for a long period of time. Arguably, that would constitute a privacy breach. That is why I think it should be specified.

Mr McDonald—There is a reason why we tend in legislation like this not to be too arbitrary about it, and that is that sometimes you might have a misconduct investigation or something of that nature where it is in everyone's interests to have the information available in that context. So usually, in similar provisions elsewhere, there tends to be an approach where you do not make it too arbitrary.

Senator STOTT DESPOJA—I am sorry, you do or you do not make it too arbitrary?

Mr McDonald—You tend not to make it too arbitrary. You usually leave it with the chief to arrange destruction, because you could get a situation—for example, an investigation into someone who is doing the wrong thing under this—where you need the irrelevant information to be kept to show that in fact the focus was the irrelevant information not the actual target. If you had something like that happening, that is a classic example of where you might want the chief to have it for a little bit longer. There are probably also other operational issues that come into it, but that is something I have certainly come across in the past—forensic procedures was one example.

Federal Agent Lawler—In the context of the broader telecommunications area, the destruction of records and how information is managed is subject to very strict and regular scrutiny by the Commonwealth Ombudsman. On the destruction of records, as Mr McDonald said, if you are too prescriptive then you find that it may work against the interests of people whom it should not work against, by not having that information available that can be both inculpatory and exculpatory in its nature. With the telecommunications interception regime, that seems to have worked satisfactorily to date. I know there are regular destruction processes. They are of course authorised by the chief executive officer, in the AFP it is the commissioner, based on reports that he receives that those sorts of issues are not likely to arise. There have been cases, I can tell you, where material has been destroyed with the very best of intent and it is unfortunate that that has occurred.

Senator STOTT DESPOJA—I guess this gets back to the debate. Mr McDonald, you brought up the words 'not too arbitrary.' I guess when you are talking about use of the word 'forthwith' to describe the destruction process, if you do not use a word like that you allow a very arbitrary or open process so that people can make decisions based on whatever it may be. But when you indicate that destruction forthwith is presumably the aim and intention, does it

not make sense to seek to define that or put in that caveat that you have described? I know the response to that is probably that you do not want to get too prescriptive for the reasons you have outlined, but I am wondering if we are looking at one argument but not the other.

Mr McDonald—The determination of 'forthwith' is totally subject to the chief officer of the agency being satisfied. That is trying to still leave him with—

Senator STOTT DESPOJA—Wiggle room.

Mr McDonald—the decision. But once he has reached the point where he is satisfied that there is no basis for keeping it any longer then it puts an obligation there. It is the old story of trying to get a balance.

CHAIR—I have some further questions about warrants, stored communications warrants in particular, but I want to move on to B-party matters, so we might put those questions on notice, if that is acceptable to the officers. Let me start with one fairly simple question about B-party warrants. I think you said in your opening remarks, Mr McDonald, that the purpose of this legislation is to implement the recommendations of the Blunn report, generally speaking. I am not going to tie you to every single sentence and every single word of the Blunn report but I am going to tie you to paragraph 12.9, which, in relation to B-party warrants, had some quite specific suggestions from Mr Blunn as to the sorts of controls and systems that should be put in place to manage these processes. We have a range of submissions—from the Law Council, the EFA, Professor Williams and even from the Office of the Privacy Commissioner—which really are quite specific and emphatic about the need for better protections, given the particularly invasive nature of the steps that are being considered in this legislation. These are pretty basic, I would have thought. I am wondering why they are not included.

Mr McDonald—Well, I have got some good news. Unlike Electronic Frontiers, who recognise that this was an amendment of a bigger bill—and you might remember we talked about the definition of communication flowing through this—a lot of the safeguards that apply to TI more generally apply to B-party and the things that are in 12.9 are covered by the rest of the TI provisions that apply. The one that is not implemented, and it is something to which we will give careful consideration, is that we have required the B-parties to be reported with the TI warrants but not separately reported. We are quite happy to say that is something that could be given further attention, because that is definitely a recommendation that we have not covered, but the rest of it is covered by general TI provisions. I do not know whether my colleagues want to add anything to that.

CHAIR—To deal specifically with the points, 12.9 states:

> ... any agency requesting such a warrant must establish to the satisfaction of the issuing authority evidence to support their belief that the information likely to be obtained from the intercept is material to the investigation. The agency should also establish that it cannot be obtained other than by telecommunications interception or the use of a listening device.

Are both of those covered explicitly?

Senator LUDWIG—And if they are, where?

Mr Gifford—The requirements for any interception warrant include that the material to be obtained from the interception of communication is 'likely to assist' in the investigation. Those are the same words that apply to B-party warrants. So we have not directly replicated the wording in terms of material to the organisation, but indeed we do have the requirement that it is 'likely to assist' in the investigation.

CHAIR—What section are you referring to?

Mr Gifford—I am referring to section 46(1).

Senator LUDWIG—You do not have the word 'material' to the investigation in there.

Mr Gifford—No, we do not have 'material' to the investigation.

Senator LUDWIG—So you have not picked that up.

Mr Gifford—We are of the opinion that 'likely to assist' is sufficient to say that there must be a nexus between communication and the investigation of the offence.

Mr McDonald—Likely but not material.

Senator LUDWIG—There is a different threshold though, is there not? Likely and material are not synonyms.

Mr Gifford—No. I would suggest that it is in terms of 'assist' and 'material to'.

Ms Hume—Also, the provision refers to what extent alternative methods of investigating the offence have been used or are available to the agency; how much the use of such methods would be likely to assist in the investigation of the offence; how much the use of such methods would be likely to prejudice—

CHAIR—Where are you reading from now?

Ms Hume—Section 46.

CHAIR—The act or the bill?

Ms Hume—The act. So when you view the B-party amendments in light of the entirety of the warrant provisions in the interception act, that is where the amendments of B-party are contained. There is a list of things on which the issuing authority must be satisfied prior to the issuing of an interception warrant, whether that be an interception warrant or a B-party interception warrant. We have included an additional test for B-party: the agency must demonstrate that it has exhausted all other practical methods of identifying the telecommunications service to be used or likely to be used by the suspect or that it is not possible to actually intercept the service being used by the suspect. That is to ensure that it is a measure of last resort and that it is done in those circumstances which are operationally required.

Federal Agent Lawler—Each of those clauses is joined by an 'and'.

Ms Hume—It is a cumulative test. That is correct.

Senator STOTT DESPOJA—Chair, is it possible to ask for an example or a scenario where you would want to use the B-party?

CHAIR—That question needs to be put in the context that, when you read the explanatory memorandum to the bill, there is not a lot of context about why we need to take such an invasive approach to these issues—why is the monitoring of people who are not suspected of anything and who have no idea they are being monitored and so on appropriate? When you take Senator Stott Despoja's suggestion of a scenario, could you also talk to us about the reasons this is necessary?

Senator STOTT DESPOJA—And why you could not get the same outcome through a name based warrant or interception.

Federal Agent Lawler—Certainly. Thank you for that question. In the first instance it is about context and about understanding where the criminal environment is and how they use telecommunications intercept or communications more broadly as a way of undertaking criminal activity. In fact, there are examples where some of the circumstances surrounding the current legislative provisions, namely, 45 and 45A, actually capture the spirit of B-party warrants. But we have an environment where people regularly use other telecommunications services.

We had one case where someone had 120 different SIM cards, and we have had cases where people have tens of handsets. Criminals, to avoid interception of their communications, will move between one SIM card and one handset. That is compounded by using friends or associates to conduct their communications so that their chances of having their communications intercepted are reduced. The broad context is that we are seeing an explosion in the use of telecommunications by a very small percentage of people to thwart what now is known as a capability by law enforcement and other agencies that work in this field.

There is the recent case of Flanagan v Commissioner of the Australian Federal Police in 1996 that related to a husband and wife situation where the service was actually in the name of the wife but the husband or partner was using that service. That is a very close example of the linkage and why B-party warrants, in issues where there may be dual criminality, come to the fore.

Where we have the situations I have described of multiple phones changing and SIM cards changing, it is often hard for law enforcement to identify the suspect's telecommunications service. Intercepting a close or known associate, somebody who we have to satisfy in accordance with the criteria you have just heard about and in the context of an affidavit before a magistrate as to what the nexus between the two is and why we believe that may produce the communications service of the suspect, is necessary.

That is in a broad criminal context. We have in a law enforcement tactical context a very different dilemma—that is, when we use undercover operatives or cooperating informants it is often necessary to have these people call particular individuals to gather evidence as to the ongoing commission of offences or offences that may have been perpetrated. That is one of the tactical techniques but as it currently stands under the law one cannot get a telephone intercept because one is required to establish that the service belongs to a person who is involved.

Of course, an undercover operative or an informant—certainly an undercover operative—will be covered by the provisions of the controlled operations legislation so we have no way

of monitoring those telecommunications real time to overcome that particular circumstance as well. So the combination of those two themes is why law enforcement is saying that this particular amendment is important and necessary.

Senator LUDWIG—Didn't Flanagan's case suggest that you already had the power?

Federal Agent Lawler—Flanagan's case is on the public record, but my understanding is that the interception, as it was put in play and authorised, did bring ambiguity and uncertainty as to the explicit lawfulness of that under the 45 and 45A provisions. Whilst the judge in that particular case did not make specific reference to or make a ruling on the legality or otherwise, effectively the evidence was produced but the judge was silent on its admissibility. Of course the evidence, as I understand it, was subsequently admitted. But it goes directly to your point, Senator, that, whilst it was utilised, there is ambiguity and uncertainty. Certainly from a law enforcement perspective, the less ambiguity and uncertainty we can have the better.

Senator LUDWIG—I did not want to debate the case, but I thought there was explicit recognition of B-party intercepts in that decision.

Federal Agent Lawler—Not that I am aware of.

Senator LUDWIG—When you read it and how section 46 is interpreted—and I do not have it with me now but—

Mr McDonald—The interesting thing about it is that it can so easily be restricted to the facts of a particular case and distinguished, but from a policy perspective we certainly need to have a decent codified position on this rather than trying to rely on peculiar facts of a particular case. The rest of the regime is codified in great detail, with relevant safeguards and the like, so I think it is desirable not only from the point of view of providing the police with some certainty in terms of their operations but also from the point of view of the safeguards and reporting aspects of it. That is one example. You could have another example where the person is a regular associate but you do not know what their regular phone number is because they keep on ditching their phones. If you know that they ring the associate, it helps you to identify what phone they are using—that sort of thing.

Federal Agent Lawler—Another example might be the recent terrorism case around the chemical stores—where you have information that somebody is going to ring in and place an order but you do not know who it is or what phone they have and the very best evidence could be obtained by such a capacity.

CHAIR—Senator Ludwig might be going on to ask this question, but what about the interception of conversations between individuals and their legal representatives or between individuals and their medical practitioners? One submission raises conversations between individuals and their clerical representatives. What about the basic concept of legal professional privilege?

Mr McDonald—In relation to that, there is the case called Carmody v MacKellar in the full Federal Court on 30 July 1997. I do not have the full citation here, but I will send that to you.

Senator LUDWIG—It goes on from Baker v Campbell.

Mr McDonald—The Federal Court held that legal professional privilege was excluded by implication under the warrant provisions of the interception act. This was—dare I say it—a member of my profession. The case involved investigation of alleged drug offences by a practising barrister. The AFP obtained TI and listening device warrants with respect to the suspect's home. They obtained a TI warrant over his mobile phone and a listening device warrant over his chambers. They did not obtain a TI warrant over the chambers' telephone. The fact that the suspect was a barrister was disclosed to the issuing judge, so the issuing officer knew that and, consistent with what I said the police would do, they did it.

CHAIR—But, Mr McDonald, if I might interrupt here, we are talking about non-suspects here, not suspects. Aren't we?

Senator LUDWIG—Yes.

CHAIR—Isn't that the point?

Senator LUDWIG—It is not only B, it is C, D and E and maybe F.

Mr McDonald—Yes. With this one, the point that was being made was that they accepted that legal professional privilege was, by implication of the act, not protected, on the basis that otherwise it would make the provisions unworkable. With these other people that might be ringing in, it still comes down to—

Senator LUDWIG—Non-suspects.

Mr McDonald—They are non-suspects. There is just no way in the world that—

Senator LUDWIG—What you are putting is this: under the current telecommunications interception regime, if you are suspected, and a TI warrant has been issued in respect of you, then under Carmody v Mackellar there is, by implication, no legal professional privilege granted.

Mr McDonald—Yes.

Senator LUDWIG—And you then say you extend that to B-party by analogy, and say that, because B-party is a telecommunications interception, in respect of the B-party—and C, D and the rest of the alphabet—they also should not be subject to legal professional privilege. But I think you are leaving out an important point with that argument by analogy. The important point is: the rest of the train is not under investigation. They are not suspected of a serious offence which warrants the privacy intrusion. That is what gives the AFP the ability to have the telecommunications interception—the balance between privacy and intrusiveness. The AFP then say, to overcome the privacy concerns of individuals, 'This person is a material suspect or is a suspect in a serious offence and therefore privacy should be reduced or diminished to allow me to do that.' In this instance, it is, I think, materially different.

Mr McDonald—The focus, though, with these is still the suspect. The reason you are getting your B-party authorisation is the connection to the suspect. So, as soon as you get to a situation where, for example, you find out what the suspect's number is or whatever, then the warrant is finished. You have not got any authority any more. As soon as you get to the point where you have collected what you need or what you were getting in relation to that suspect then there is no basis for the warrant. The only exception to that is where you find out that that person is actually incidentally involved with a suspect.

Senator LUDWIG—But then they become suspect and part of the ongoing investigation and you would go back and get a telecommunications interception warrant for that person, in any event, to overcome that problem. Therefore you do not have a problem with use or derivative use in that respect. If that is your argument then you should not have a problem with that either, because it is only up to that point. It is about identifying the original source, as a last resort; identifying the handset; tracking your officer—

Mr McDonald—In that particular example, it is.

Senator LUDWIG—It is in all the examples we have been given—unless your officer is up to no good. And I do not believe that.

Federal Agent Lawler—Thank you, Senator. In the example of the chemical company, you could have a hypothetical situation, or maybe not so hypothetical, where—

CHAIR—We are happier dealing in hypotheticals!

Federal Agent Lawler—Indeed. With suspected purchases of explosive chemicals that are outside the norm, a particular chemical company has come forward and advised us that a particular person will call in. He does not know who the person is. He might have given a name; it could be false, but they will ring in to the chemical company and advise delivery and other sorts of details et cetera. The B-party warrant in that situation, given the current legislation, says that the person must be involved in the offence. That is the link back to being able to establish a telephone intercept. Quite clearly in that case—

CHAIR—Which clause are you reading from?

Federal Agent Lawler—I am reading from my briefing material.

CHAIR—Mr Colvin will be able to tell me which clause it is.

Federal Agent Colvin—I will refer that.

CHAIR—For answer today? It was not that hard a question.

Federal Agent Colvin—To answer today.

Federal Agent Lawler—It is under the Telecommunications (Interception) Act 1979.

CHAIR—So we are still dealing with section 46 of the act. I thought you were reading from a new clause.

Federal Agent Lawler—The point I am making is that it relates to the person being involved in the commission of the offence, or reasonably suspected of being involved.

CHAIR—Why would you need a B-party warrant if you are dealing with the chemical shop owner? Wouldn't you just use a named person warrant?

Federal Agent Lawler—The chemical shop owner may, for a whole variety of reasons, not wish to cooperate.

CHAIR—But they have rung you. You said they rang you and said—

Federal Agent Lawler—It could be that they rang a reporting line of some sort or advised the police in some method and said: 'We don't wish to be further implicated here. We want to remain anonymous, but this is a difficulty that I have, and here it is, for what it's worth.'

CHAIR—I am confused.

Mr McDonald—I think the point he is making is—

CHAIR—They have rung 1800 123 400, which I like to put on the record repeatedly because I know the number, and said—

Mr McDonald—People are worried about people taking revenge attacks and things like that. That would be a factor, wouldn't it?

CHAIR—I do not think they need to put an ad in the front of their shop.

Senator LUDWIG—'I have a telecommunications interception'!

CHAIR—To be serious for a moment—for an extended period probably—we are having some difficulty with the rationale and the management. I ask about protections; you tell me it is okay, the protections are built in, but this is ramping up the degree of intervention and exposure of people's privacy to an extraordinary level. This is not your average named person warrant or your average intercept; this is an interception on another party who is not suspected of anything at all. In fact, it is probably on more than one party, depending on how the hypothetical progresses, let alone the reality. So I think you will find, Mr McDonald, that the committee is concerned about 'superprotections' for individuals, their privacy and their civil liberties in this process—persons who are not suspected of anything.

Mr McDonald—Remember also that the fundamental threshold in this is that the provisions are not used unless normal methods cannot be used.

Senator LUDWIG—Or are exhausted.

CHAIR—Can you tell me where it says 'last resort' in the bill? 'This is a measure of last resort'—where does it say that in the bill? I do not want to be told it is in the substantive act and get that wrong again, so I am going to rely on you to explain it to me.

Ms Hume—Schedule 2 of the bill does refer to having 'exhausted all other practicable methods'.

CHAIR—Is that what it means?

Ms Hume—It is an amendment to section 46 in schedule 2. I refer you to the test which is—

CHAIR—'The Organisation has exhausted all other practicable methods of identifying'—is that the one you are talking about?

Ms Hume—Yes, that is correct. Both in amending section 9 and in amending section 46, we refer to having 'exhausted all other practicable methods of identifying the telecommunications services' of the suspect or person of interest or it not being possible to intercept the telecommunications service of the person of interest or suspect.

CHAIR—We are not sure that we agree that that equals last resort, to be honest with you.

Federal Agent Lawler—Could I make a point of clarification around those examples. I think there might have been a misunderstanding that one can consent, as in the chemical store owner can consent to a telephone intercept. They cannot consent.

CHAIR—My question was about a B-party warrant; if you knew the store owner and so on, you would be using a named person warrant—

Senator LUDWIG—For a named person or part of the investigation then you can use a TI warrant, and you would then go to the issuing authority.

CHAIR—We were not thinking you just put up your hand—

Senator LUDWIG—That is not publicised either.

CHAIR—I think we understood where you were coming from.

Ms Hume—If I may assist, particularly with undercover operatives, and where someone has consented to their phone being tapped, they are not committing an offence under which a telecommunications interception warrant could be issued—that is, a seven-year offence or more. In that case, it would not be possible to intercept their telecommunications but for the new test in (3B) under section 9 or how we are amending section 46. So where it is not possible to otherwise intercept the telecommunications service of a suspect or person of interest in that case—because they are not actually committing an offence—it is not possible and therefore B-party warrants would be used in those circumstances.

Senator LUDWIG—That does not equate with last resort. It is just that they are not committing an offence.

Mr McDonald—When we are talking about last resort, we are making the reference to this 'exhausting all other practicable methods'. That is what we are referring to.

Senator STOTT DESPOJA—I think you have managed to put on record quite effectively the concern that has been expressed in submissions and in the committee in relation to nonsuspects generally or nonsuspects who may have a profession that attracts a privilege—whether it is legal professional privilege et cetera—but I would like a definitive response as to whether or not schedule 2 abrogates legal professional privilege. Does it completely override it, as some people suspect it might or as the Law Council asks if it does?

Mr McDonald—If you read the cases on legal professional privilege, including Carmody and MacKellar, the general rule is that you have to expressly exclude legal professional privilege. In this case, they said that the statute itself strongly implied that the warrant provisions overrode it. But that is in the context of that particular situation.

Senator LUDWIG—Your view then is that, in terms of how B-party would operate, legal professional privilege is not an impediment to collecting that information.

Mr Gifford—Not to the initial recording of that information. When you went to court to try to use that information, it would be tested by the court as to whether or not legal professional privilege applies. There is no express abrogation of legal professional privilege by the act.

Senator LUDWIG—But it would go to the point that you could get a B-party intercept against a lawyer, record the relevant conversations, and then it would be up to the lawyer concerned to argue that a particular part of the conversation, or all of the conversation, was protected by legal professional privilege and the case would turn on whether it was advice that he was providing or whether it was something else.

Mr McDonald—The big problem we have got with this is that some of these professions are involved, and in a practical sense it is really the only way in which—

Senator LUDWIG—But if that is the case then you can get a telecommunications interception warrant. You do not require a B-party intercept, because a B-party intercept is for a nonsuspect.

Mr McDonald—In this case, the person is not a suspect; they are discussing it with a suspect. If you had some sort of notice, for the purposes of legal professional privilege or something like that, all you know is that that person is associated with the suspect. So, especially with some of these more dangerous investigations, you would be worried about tipping off the suspect. This is an area which raises a lot of practical issues. On the other hand, we are recognising that people are beginning to avoid this sort of interception. Surely, at the end of the day, what we have is the best result—the person can still raise privilege, should they want to use the evidence.

Senator STOTT DESPOJA—I am interested in your comments, Mr Gifford, because I understand from your response—and I think we all now understand it—that, regardless of the intent, based on legal precedent and the legislation, legal professional privilege is effectively overridden?

Mr Gifford—No.

Senator STOTT DESPOJA—I am interested in your comment. I am not quite sure whether you said it is not expressly written—and obviously that is one of the recommendations which we are dealing with—and whether to expressly put it into the act. I know, Mr McDonald, you are talking about professions. I am trying to specify—obviously based on the submissions of the Law Council and others—that it is not just a practical argument; that argument is a key professional, ethical issue et cetera. So, restricting it to the issue of legal professional privilege, can you clarify it for me?

Mr Gifford—I will try to be as clear as I possibly can. In terms of the case of Carmody, Carmody said that the application of a telecommunications interception warrant implicitly abrogates legal professional privilege so that communications could be recorded. Legal professional privilege still exists to the extent that it is to be tested before the court whether or not those recordings are admissible.

Senator STOTT DESPOJA—Obviously, the Law Council comes back with Baker v Campbell in relation to the effect that that has. I understand that point. In your original comments you used the term 'expressly written in the act'. Would it be problematic for this legislation to expressly state that schedule 2 does not override legal professional privilege?

Mr McDonald—That is probably something that we will take away and give a considered response to.

Senator STOTT DESPOJA—Okay.

Senator LUDWIG—It would certainly help to make it plain in the sense of how you expect B-party warrants to work. You are taking a belt and braces approach to make it plain that it is permissible. The additional matter, of course, that you raised in your answer was about, effectively, B-party warrants being a fishing expedition by lawyers. That is what I

worry about as well: that B-party warrants will not be used as a fishing expedition. Blunn said that it should not be used as a fishing expedition, and if the person is a nonsuspect then it should only be for limited and controlled purposes. That is what Blunn said. What I have difficulty in understanding and hearing from you and when I read the amendment is that it does not look as though it is for a limited and controlled purpose. It does seem to be—and from the evidence you have provided—a fishing expedition. I am sure the AFP would not agree that it should be. I hope to hear from them that it will not be used as a fishing expedition. But the possibility is there. I am trying to ensure that there is not a possibility.

Mr McDonald—The threshold for the issue of these warrants is certainly focused on the original suspect whom you are investigating. Even under the current system, when you have an intercept on the suspect, you have various people talking to that suspect—either the suspect is ringing them or they are ringing the suspect—it is possible that innocent people can be intercepted here and now in those circumstances, as a result of something they say or innocent flags going up. So, essentially, this is the reverse of that situation. I think the threshold that we have here that starts the whole process is such that it would be extremely difficult to have this as a fishing expedition if the police were so minded, and I know they would not be so minded. It is all about whether they have exhausted all other practicable methods in relation to the person involved in the offences.

CHAIR—I have to say I think, if it is the reverse of the situation you describe, Mr McDonald, it is not going to win a gold medal at the Commonwealth Games for a reverse pike with thrust! It is not; it is quite different. Seriously, it is quite a different situation to what you were talking about. This is incidentally collected information derived from a telecommunications interception placed on a suspect versus a telecommunications intercept placed on a nonsuspect on purpose.

Mr McDonald—But the focus of placing it on the nonsuspect is to get at the suspect—

CHAIR—I understand that.

Mr McDonald—just in the way that the regular one is focused on the suspect as well. The grounds are such that they force the police to focus on the suspect, otherwise what they are doing is going to be brought into question in court and they will say it is illegal.

CHAIR—And I interrupted Mr Lawler who was just about to say something.

Federal Agent Lawler—I was firstly going to respond to Senator Ludwig and make the confirmation that the AFP does not go on 'fishing expeditions'. Furthermore, I want to say that, in these sorts of circumstances, what we will have to do is to establish with the judge or the issuing authority the nexus between the two. These sorts of circumstances arise and it may well be that there are telephone intercepts in place on a particular suspect. It is quite clear from an AFP perspective and a resource perspective that is where we would want to focus the investigation because that is where the principal evidence will come from. But where we get the sort of activity that I have described, the use of multiple phones, phones being discarded, SIM cards being changed and other sorts of activities deliberately directed towards interfering with the investigation, if you have already an established—this, of course, is based on the facts and what is presented to the judge—and clear associate where you know there is communication regularly occurring then it gives the investigation a very clear avenue to be

able to direct its focus back onto the suspect again. This is in that first theme of reasons; this is one of the major practical difficulties that we find.

Senator LUDWIG—It could also be a private residence, a household with a family of six where you are waiting for Johnny to phone home.

Federal Agent Lawler—As Mr McDonald and his colleagues have said, when you look at the criteria that one needs to establish, one important thing that has not been mentioned and which is at the top of my briefing paper and I understand also in the act is how much the privacy of any person would be likely to be interfered with by the interception as a start point. The act goes on to address the gravity or seriousness of the offences being investigated, and how much the intercepted information would be likely to assist with the investigation by the agency of the offence. It continues with to what extent alternative methods of investigation of the offence have been used by or are available to the agency, and how much the use of such methods would be likely to prejudice the investigation by the agency of the offence. That is predicated by some additional criteria at the start of the Telecommunications Interception Act, which also apply. So, in the context of the facts being presented to a judge meeting these criteria, whilst people can say it is a' fishing expedition', really when one has to look at it objectively as to what you need to satisfy, I question whether that holds a lot of water.

Mr McDonald—The judicial officer is going to be really suspicious of that. They are going to the testing of the application with that in mind.

CHAIR—What is the Attorney-General going to say to ASIO when it is the Attorney-General to whom an application is made?

Mr McDonald—The Attorney-General has always issued TI warrants.

CHAIR—I did not get far on that matter with the Law Council this morning. It was a matter of some frustration for me, but that is neither here nor there; it was early. I understand that absolutely, but the Attorney-General now also has the capacity to grant B-party warrants, as I understand it—or did have.

Mr McDonald—I was going to say, in finishing off that point, that not only do the AFP have to then worry about this being tested in court but they have also got the Ombudsman overlooking them. A person can make a complaint to the Ombudsman at any time. ASIO have got the Inspector-General of Intelligence and Security monitoring their situation. The Attorney-General has had the role of being responsible for issuing these warrants, in the case of telecommunications interception warrants, and other examples—which the Law Council could not remember—include the authorisation of ASIO questioning—

CHAIR—That is what I wanted to go through this morning.

Mr McDonald—So the Attorney-General has always had that sort of responsibility. As for this case, I think, if it were shown that that power was not used judiciously or whatever then he would find himself open to criticism which would be severe political embarrassment. On top of that you have got the independent Inspector-General of Intelligence and Security looking at the ASIO processes themselves. I think we have got a system here in Australia which has a lot of safeguards in place.

CHAIR—There are two things that I want to say about the Ombudsman and the IGIS before questioning goes back to Senator Ludwig. The first is that I am not entirely persuaded that one can complain to the Ombudsman or the IGIS about a telephone intercept that one does not know about. That would be one small technical problem. The second is this: if you have had a chance to look at the Ombudsman's submission, you would have seen that it is a broader issue than just the B-party warrants. The Ombudsman is quite apprehensive about what this opens up as to the work that the office will be required to do and the role they will be required to fulfil. So it is important to place on the record, from my perspective—and perhaps from the committee's perspective in due course—that I take the Ombudsman's submission on those matters extremely seriously.

Senator LUDWIG—The Privacy Commissioner goes on to say, on page 2, in relation to B-party intercepts:

> Such parameters may include enforceable prohibitions on the use or disclosure of intercepted material for any purpose other than the purpose stated in the warrant; and enforceable, audited requirements that any intercepted material outside the scope of the purpose stated in the warrant be immediately destroyed.

What do you say about that?

Mr Gifford—The use and destruction provisions that are currently in the existing Telecommunications (Interception) Act will apply to B-party interception. It was a conscious decision by the Attorney-General that they would be maintained. The Attorney has been made aware of all submissions to this committee and will consider any submission on that basis.

Senator LUDWIG—In terms of that particular matter, you are going to rely not on an immediate destruction of material that could be collected outside of what otherwise would be necessary for the investigation. How long would it sit on the record for?

Mr Gifford—The Telecommunications (Interception) Act currently requires the destruction of material once the general and special registers of warrants have been inspected by the Attorney-General. Those registers are compiled three-monthly by the AFP. After they are reviewed and signed off by the Attorney-General then a notice is provided to all agencies, at which point they may destroy all material that is contained in the general and special registers.

Senator LUDWIG—How long does it take you to destroy material after the three months?

Federal Agent Lawler—I might need to take that on notice. I do not know that there is a definitive answer there. I think it would be an answer that we would need to just look at and see what factors impacted upon the destruction process. I know it is a matter that the Ombudsman looks at and examines on behalf of the AFP. Certainly, from my limited experience, I know that we do that expeditiously once the appropriate destruction procedures have been complied with—but, as to whether that is in hours or days, I would need to come back to you. It may well be that in some jurisdictions or some parts of the AFP, it might be X amount of time and in others Y and there may be very good reason for that. I am happy to try to give you a fulsome explanation of that.

Senator LUDWIG—That would be helpful. Another of the senators has raised the issue of use and derivative use. At the moment your position is that there would be use and derivative use of the material.

Mr McDonald—Yes.

Senator LUDWIG—If it is a non-suspect, why do you require use?

Mr McDonald—The circumstance where it could be used might be one where the person started out as a non-suspect. I know this will get you worried about fishing again, but the practical reality is that sometimes you might think this person is providing groceries to personal suppliers or something like that and it works out that they are actually supplying the person with something else. The situation is going right back to the search warrant provisions themselves. When you are searching someone's house, if you go in there with a proper suspicion that the person whose house you are searching has committed a crime and you find that the flatmate has got a heap of stolen goods in his room, is attending the drugs that he is growing or something like that, the police cannot turn a blind eye to that situation. There would be circumstances where it is necessary to use it.

Senator LUDWIG—What happens when you get to (c), (d) and (f), though? It is not actually the non-suspect or the B-party. It might not even be part of the original offence; it might be some other—

Mr Gifford—This is consistent with the way that a service or named person warrant currently operates: you may be the target of the interception and conversing with Senator Payne, and Senator Payne is not a target of the investigation at all. But Senator Payne may talk about another offence that was not the subject of the original investigation, to the extent that the original warrant was justified to and authorised by the issuing authority. Then any criminal intelligence which is subject to a three-year penalty threshold can be used.

Mr McDonald—And Senator Payne might in turn implicate someone else.

Senator LUDWIG—Or someone else could be using her telephone service and implicate themselves in a serious offence.

Mr Gifford—The reverse situation would require destruction of very valuable criminal information. The extreme example would be that you would happen upon some very valuable information in terms of a terrorism investigation. That is an extreme example, but the use of that information is useful for our operational agencies and has been justified in terms of the initial warrant being authorised by the issuing authority.

Senator LUDWIG—I think what concerns people, in terms of the submissions they make, is that it is the primary target that is a non-suspect to begin with.

Mr McDonald—Right from the word go we have recognised that that is a very serious issue, and we are not at all surprised that people are concerned about it. However, we are facing a practical problem which some law enforcement agencies are very concerned about. It is due to people becoming more savvy about these matters. People are obsessed with telecommunications nowadays. You cannot go anywhere without seeing someone walking with a mobile phone at their head or something like that. People are savvy enough now, if they are involved in the criminal side of things, to use the technology. It is a difficult situation,

but the grounds for getting this type of interception are such that it is focused and should not be easy to get, particularly given that we have an independent judicial officer issuing it and being fairly aware of this. It is very difficult to see how you can design it much differently without undermining the practical objectives behind it.

CHAIR—May I ask, Mr McDonald, how you regard the suggestion made by Professor Williams that the bill should require, as a precondition to issuing a warrant under proposed section 9, that there be evidence that the B-party's telecommunications service is likely to be used to communicate or receive information relevant to the particular activities prejudicial to security which triggered the warrant.

Mr McDonald—We already have to show that information that would be obtained by the interception would be likely to assist in connection with the investigation by the ANC of a seven-year offence, which is suspect—

CHAIR—But that is not about the use of a telecommunications service itself.

Mr McDonald—It is information that would be obtained by interception, so it is referring to the particular interception. We have all the other stuff that Mr Lawler read out on the grounds, so I think there is more than enough. Given that Professor Williams was coming from a point of view of not looking at the particular proposed section, I would say that when he sees that section he will probably be pretty happy about it.

CHAIR—Who will be happy?

Mr McDonald—Professor Williams, because that proposed section has—

CHAIR—You might find Professor Williams has seen the section, but you were here for that evidence. Mr Lawler, do you want to comment on that suggestion?

Federal Agent Lawler—Yes. My initial reaction is that there would be circumstances whereby that could very well be too narrow from a practical operational perspective—not wanting to regurgitate what I have previously said—and could be a restriction on law enforcement that, given the other safeguards, in my view does not strike the right balance. This is all about balance and, of course, different judgments on where that balance is properly placed.

CHAIR—I suspect Professor Williams is looking for narrow.

Federal Agent Lawler—Indeed, he was.

Mr McDonald—He might have been, but I think he said at the start that he was not totally across it all.

CHAIR—No. He said he was not an expert.

Senator LUDWIG—He always says that.

Mr McDonald—He is very modest. Quite a few people missed the relationship to proposed section 46 and everything that is in it.

CHAIR—You say that again, Mr McDonald, but the point is that they have not missed the relationship to proposed section 46 and neither has the committee. What the witnesses have been concerned about, and what we have been listening to, is the fact that this is regarded as a

substantial extension of powers to invade people's privacy. That is a significant concern for which proposed section 46 is not regarded as an entirely adequate set of protections by some people. I understand that does not include you. We have been through the finer details of proposed section 46 at some length. But it is other people's view, and the committee has been listening to that—and to you.

Mr McDonald—But on the likelihood front—I know I am raving on about it—because this relates to the interception of a B-party, these grounds are actually quite useful in providing the sort of safeguard that Professor Williams is talking about.

CHAIR—Perhaps I need to find myself a judge or a member of the AAT who will talk to me about how much they take into account the privacy of any person or persons who would be likely to be interfered with!

Mr McDonald—It is a big issue with a lot of people.

CHAIR—It is an interesting question for the committee because that is not something we are in a position to inquire into, to the best of my knowledge.

Senator LUDWIG—Was the submission about B-parties originally a request to Blunn from the AFP in their submissions? Where did it originate?

Mr Whowell—So as not to mislead the committee, I would have to check our original submission. It has been some time since I have looked at it. But I think it was an issue that had been around, and I believe we touched on it.

Mr McDonald—It came up in ongoing consultations with various law enforcement agencies—including the state ones, of course—so it could have come up in quite a few contexts.

Ms Hume—And he was aware of the decision in Flanagan and Grollo, which he specifically refers to in his report. He was aware of that decision and the implications that that has for our warrant provisions in the act.

Senator LUDWIG—Perhaps you could take that on notice. The last question is: do you rely on any overseas precedent with B-party warrants and how they have been used? Are you familiar with any?

Mr McDonald—The US, for example—and Mr Gifford will correct me if I am wrong—have quite open arrangements to do with a whole block of organised crime activities, so they have what is not a terribly prescriptive system. They would be able to, just on one warrant, intercept a whole heap of people that are associated with a particular person.

Mr Gifford—We would be happy to provide an international comparison, with the UK and the US at the very least.

Senator STOTT DESPOJA—Especially in light of Professor Williams's comments, because I think he made the point that individual legislation should not necessarily be judged without the context of or backdrop to any legislation passed in, say, a jurisdiction like the UK—

Mr McDonald—The system for stored communications, for example, in the UK—just to beat our drum for a change!—is a lot more open-ended than what we have. So, contrary to

what Professor Wiliams says, referring to a country that can detain people with preventative detention for 28 days rather than what we have—

Senator STOTT DESPOJA—He did talk about the backdrop, Mr McDonald, of a human rights act or a European human rights act, or a bill of rights in the case of America.

Mr McDonald—It does not change the situation. You have to look at what the law says.

CHAIR—Indeed. I am acutely aware that I have another witness after we conclude with the AFP and the department, so I do want to move on to a discussion as brief as we can make it on equipment based interception under schedule 3. I think that is the last major area of concern.

Senator STOTT DESPOJA—Chair, can we just clarify what provisions have been made for questions on notice, because I am happy to—

CHAIR—They need to be put on notice as soon as possible and answered as soon as possible.

Senator STOTT DESPOJA—Right. I was just thinking about putting some questions on notice, but I am happy to do that and to deal with this very briefly. I do have one question, though, that is about schedule 6, the other bits, and that would probably be very quick if you wanted me to get it out of the way.

CHAIR—Okay. Ask the 'other bits' question now.

Senator STOTT DESPOJA—As the department is probably aware, the *Bills Digest* raised some issues for the Senate in relation to retrospectivity. I am assuming you would suggest that they were technical amendments and not a big deal, but I wanted to clarify that in relation to item 8 and item 3—somewhere around here.

Ms Hume—That is—

Senator STOTT DESPOJA—I know what I am talking about! Could you just tell me whether I should be worried?

Ms Hume—I understand exactly what you are talking about, Senator. It is in relation to the Office of Police Integrity in Victoria. There were amendments made to the interception act late last year to do with making that office an eligible authority for the purposes of the interception regime. Those provisions, however, will not commence until the Attorney is satisfied with the oversight regime that is in place in Victoria. They will not become an eligible authority before that. Therefore, those provisions are yet to commence.

The amendments that we are making in schedule 6 in our bill, which refers to the Office of Police Integrity, will not commence until those provisions commence. They commence immediately after the provisions that were amended in the act in relation to that office last year commence. It is a long way of explaining it. There is no element of retrospectivity in relation to extending the permitted purposes that the Office of Police Integrity may have if those provisions do actually commence.

Senator STOTT DESPOJA—And the second example was one in relation to the effective decisions of the District Court of South Australia.

Ms Hume—That is right—the decision in Sutton and Rogers. It is a validation provision. We are actually amending the provision in the Telecommunications (Interception) Act to allow, and which always has intended to allow, an employee of a carrier to assist law enforcement in interception when a warrant is served. An employee of a carrier actually conducts or assists that interception. That was challenged in Sutton and Rogers. The provision is a validation provision. It will commence retrospectively so that all activities under interception warrants that may be called into question because of that decision will be validated. That was explained in the EM, and I understand that the scrutiny committee was satisfied with that explanation.

Mr McDonald—It is extremely remote that that case would have that result, but we are just tidying it up.

CHAIR—We will now move on to equipment based interception. We will spend a brief time on this, and then we have to go to our next witness.

Senator LUDWIG—It is really only an issue that the EFA raised, and it is also reflected in Blunn. The Privacy Commissioner similarly mentioned it. Presently, there does not seem to be an ability to uniquely identified equipment. It seems that the handset can have multiple numbers, or at least not be able to be identified as unique. In 3.2.3, Blunn indicated:

> Whatever the solution it would be imperative that some system be devised which provides for the effective identification of the means of communication.

In other words, there was not an effective means in place. The EFA's concern—I am using a shorthand method—is that this is not a way of uniquely identifying a handset as there is no way to do so, and, therefore, it is broader than that, because you might capture multiple handsets.

Mr Gifford—We do understand that risk, and we are aware that there are duplicate IMEIs in a telecommunications network. On that basis, we have said, 'When you're seeking interception on the basis of a handset, it must be defined by reference to a unique telecommunications number, which, for the purposes of the definition, will include an IMEI.' The reference to say it must be a unique number means that where in a pre-execution of warrant inspection it is identified there are duplicate IMEIs on a network, interception will not be allowed. You must satisfy the issuing authority that the IMEI you are seeking interception of is a unique IMEI number.

CHAIR—How do you do that?

Mr Gifford—It is through a pre-warrant—actually, I will defer to the AFP on the matter of pre-warrant.

Mr McDonald—There will be no doubt be situations where there is—

Federal Agent Lawler—My understanding is that the IMEI number is a unique identifying number, but we have seen a practice whereby these numbers have been copied fraudulently within service providers to commit fraud, but also to enable another way of not being able to identify who has the particular handset in question. I understand from the briefings I have received that there is the capacity to remove such duplicate numbers from the system, as there is also the capacity to remove stolen handsets from the system. As has been

indicated, we would do the checks that are required for the potential for those numbers to be duplicated on the system, but they are only duplicated through, as I am briefed, a fraudulent activity and the numbers being cloned or copied.

Mr McDonald—I think we passed an offence to do with that a year or two ago.

Federal Agent Lawler—We did.

Senator LUDWIG—What the EFA say, though, is:

... there is no requirement that the "telecommunications number" (or "other identifying factor") of the "telecommunications device" be advised to the issuing authority, nor any requirement that the issuing authority be satisfied that the device can, in fact, be uniquely identified by a number.

Ms Hume—Proposed section 6Q in schedule 3—it is page 64 of the bill—talks about the identification of a telecommunications service. In both subsections (a) and (b) it refers to a unique telecommunications number. In item 3 the list of those numbers shows that potentially it could be a telephone number. It could be an IMEI, as Mr Gifford explained. It could be a MAC address of a computer. But that provision, 6Q, specifies that it has to be unique; it is a unique telecommunications number.

Senator LUDWIG—How will the AFP know that?

Mr McDonald—That is best answered by the AFP.

CHAIR—I think that was the plan.

Federal Agent Colvin—We would make all efforts we could to ascertain that through our inquiries to the telecommunications companies. The concern, of course, is that some of these are fraudulently obtained. A number of different identification numbers can be applied to that communication tool, be it a telephone or a laptop computer. I could not give you one answer now that would tell you how we would do it across the board, but we would have to go to a range of telecommunication companies to ascertain whether these numbers are being used somewhere else or whether they are unique to the person, phone or laptop that is of interest to us.

Senator LUDWIG—But when you appear before the issuing authority you have to say that it is a unique identifying number.

Federal Agent Colvin—We would have to; that is correct.

Senator LUDWIG—How do you demonstrate to the issuing authority that you have done that research?

Federal Agent Colvin—We would have to outline to the issuing authority what steps we have taken to satisfy ourselves that that number is a unique number.

Senator LUDWIG—Is there a requirement in the warrant for that?

Federal Agent Colvin—In the affidavit?

Senator LUDWIG—Yes.

Federal Agent Colvin—I would have to check.

Federal Agent Lawler—There is a requirement to the extent that the affidavit is constructed to meet the particulars of the section.

Mr McDonald—Yes, that is right. Again, this is just a matter of proof. Our hope, of course, is that this is an area where, over time, we can get better and better. The reality is that we have set a bar there which is going to require the AFP to demonstrate to the issuing person that in fact it is unique.

Federal Agent Colvin—In doing so we would have to demonstrate how we arrived at the conclusion that we have this number.

Mr McDonald—Yes.

Federal Agent Colvin—So it is implicit that we would have to step through why we say that this number is the number we are interested in.

Senator LUDWIG—If there are other matters I will put them on notice.

CHAIR—There were some concerns raised by the Privacy Commissioner about this schedule and its operation which we will place on notice, some of which are also reflected in other submissions. I suspect there will be some requests for answers to questions on notice. As you know, the Senate requires us to report by 27 March, so we will turn the questions around as fast as we can, if you would be kind enough to turn the answers around as fast as you can.

Mr McDonald—Yes, and we will get those loose ends back as quickly as we can.

CHAIR—I thank all of the officers who have been present this afternoon. We appreciate your assistance. Federal Agent Lawler and the AFP, Mr McDonald and the Attorney-General's Department, thank you very much.

[4.19 pm]

BIBBY, Dr Richard Martin, Assistant Secretary, New South Wales Council for Civil Liberties

MURPHY, Mr Cameron Lionel, President, New South Wales Council for Civil Liberties

CHAIR—Welcome. The Council for Civil Liberties 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 Murphy—No.

CHAIR—I ask you to make an opening statement and then we will go to questions.

Dr Bibby—Thank you for your invitation both to submit and to appear—it is appreciated. We are pleased with the bill in certain respects: it increases the extent to which privacy considerations must be taken into account in relation to class 1 crimes, the attempts to limit the possibilities of abuse and the need to consider alternative methods if they are reasonable and to consider whether alternative methods of policing have been tried. We are glad of these but they all need to be strengthened because it is patently obvious that warrants are issued far too readily. Specifically, on stored communications, much of the debate seems to have been on whether they are sufficiently different from interceptions of spoken communications. We have not seen, nor have we heard today, any account that makes sense of the notion that they are any less private. The second reading speeches talked about them being somewhere in the middle but no reason is given. It is absolutely absurd to say that because they are more considered messages they can be treated differently. They are just as private and one may, in completely considered fashion, type in an SMS message, 'Dad, I'm in trouble', or 'I need your desperately,' or 'I'm considering suicide,' or whatever. They are still private matters. If you watch the flying fingers of a teenager on the train, you see that there is no stopping at all for consideration.

B-party warrants are the most concerning thing about this. They are contrary to the International Covenant on Civil and Political Rights, as an invasion of privacy, and ultimately they are futile. Getting around them will just be a matter of ingenuity. It is not very hard to think up ways that you could get around them. This privacy means nothing when a law enforcement agency wants to invade and some limit must be set. We think that is where the limit should be. B-party warrants are unacceptable. If that view does not prevail, then what needs to be said is that they should be limited to saving lives. At the moment, it is nothing like that. The seven-year penalty threshold covers a great many other matters indeed. If the B-party warrants were to proceed, then we think that threshold should be where life is at risk or where life has been taken. That way, you catch real terrorism offences and you would catch murder cases, I guess.

Mr Murphy—I will quickly add to that by saying that the entire purpose of the Telecommunications (Interception) Act is to protect the privacy of people using communications devices. It makes it an offence for someone to do so without obtaining a lawful warrant and the concerns that this amendment raises are that it is a massive expansion of the invasion into people's privacy who use telecommunications devices while at the same time there is no real justification for that. We can accept that, if someone is a suspect in a

criminal investigation, it is a matter of balancing the interests of the public in ensuring that that suspected offence is investigated and that the person is prosecuted and dealt with under the law. In this amendment, we are dealing with something that goes much further than that. We are talking about innocent B-parties, people who are not themselves suspected of any offence. The whole regime of B-party warrants really shifts the focus of the investigation from someone who is a suspect to an investigation surrounding the innocent B-party on the off-chance that a suspect might contact them and there might be useful information gleaned that way.

There really is no logical reason why you would need a B-party warrant. It appears to us that any of the evidence sought by law enforcement agencies could be obtained through an ordinary service warrant or a named person warrant. We have not yet seen a single example that stands up to even basic scrutiny about why a B-party warrant might be needed in order to obtain evidence about the suspect. Of course, having a B-party warrant in place means that the B-party may lose professional legal privilege. If they are a lawyer, everybody who communicates with them is going to be recorded and transcribed, even though it may not be used in later prosecution. Many people make intimate, private calls over a phone line to family members, a loved one or a medical practitioner, where they might be discussing a deep and traumatic illness. These are exactly the sorts of things—and the privacy—that are going to be invaded through the use of B-party warrants.

To suggest that there is a sufficient system to deal with this through the Ombudsman inspecting and being there as a mechanism of complaints ignores the fact that these warrants are covert—the person does not know that there is a telecommunications interception warrant in place and they do not know that their privacy is being invaded. They cannot, therefore, go to the Ombudsman and complain and say, 'I am upset with this and I want something done about it.' I will not take any more of the committee's time. I will leave it there, but we are happy to answer any questions that you might have.

CHAIR—Thanks, Mr Murphy.

Senator STOTT DESPOJA—Your final recommendation, Dr Bibby, relates to the committee resisting attempts 'to give powers to make decisions that permanently or significantly' et cetera. Essentially you are arguing that we should resist it when it comes to affecting the fundamental rights of any individual. Obviously that is a message for us in relation to this specific legislation, but I am wondering if your organisation has a view as to the operation of this bill when you put it into the context of legislation that has been passed in recent times. I am interested in the cumulative effect of the legislation, particularly how this legislation will operate in conjunction with antiterrorism legislation and surveillance legislation—all of those bills that have been passed in recent times. What impact is this having on the privacy rights of Australians?

Dr Bibby—One of the most obvious matters concerns the Citizenship Bill before the parliament which, if passed, will give ASIO the power to deny an application for citizenship without even the Attorney-General having the right to override it. It is an extraordinary power. If ASIO gets information from interceptions which are not able to be checked or answered by people and if ASIO starts to behave in the way ASIO used to behave in the past—I think it is susceptible, for reasons which are in the submission—then people will be denied the right or

the opportunity to become Australia's citizens, for bad reasons. Any invasion of privacy, and especially a secret one, runs the risk of misinterpretation of the materials. It is a standard objection, of course, to collecting information and keeping it secret or putting pieces of information together unless the person is able to see it. That is the reason why the Australia card was rejected in the past.

As soon as you give powers to organisations to take away liberty in the way that the two antiterrorism laws and the powers that were given to ASIO a few years ago have done, you open up the possibility of it being done for totally spurious reasons. The more you allow privacy to be invaded, and the more you allow the stuff to be kept secret, the greater the chances are that these powers will be misused—and misused in ways which it is impossible for people to correct.

Senator STOTT DESPOJA—Do we have the balance right at the moment?

Dr Bibby—No. And what does balance mean? It is not just a case of fiddling—

Mr Murphy—You might look at in this sense: in the context of all of the recent measures that have taken place, what we are seeing generally is a situation where we are told that certain extraordinary powers are required because there is a specific threat—a terrorist threat is the example that has been used in the context of the antiterrorism legislation—and that justifies a departure from the norm. So, instead of maintaining privacy, there is an imminent threat and we need to deal with it. We are seeing both the public and the parliament becoming desensitised to the nature of the extraordinary powers that are being sought. Instead of just being used to get us over a period in which there might be a drastic and imminent threat, it is becoming the norm, and those powers are being extended to many other agencies. There are not sunset clauses that would remove them after a particular period. This also, in a sense, is part of that process in which we see B-party warrants being asked for without any example that stands up to any scrutiny.

Senator STOTT DESPOJA—On that point, what did you make of the deputy commissioner's example?

Mr Murphy—The chemical plant?

Senator STOTT DESPOJA—Not just that specific, albeit hypothetical, example. Can you envisage a circumstance where the AFP have a point and that they could not necessarily obtain the same outcome with a name based warrant or an equipment based warrant?

Mr Murphy—I cannot. The real point is that it is not for the rest of us other organisations to try and justify these powers; it is really a burden on the agencies that are asking for them to establish why this is necessary. But all of the examples that have been raised, when they are put up to basic scrutiny, do not stand up to that scrutiny. With the hypothetical chemical shop owner, it appears to me that there is no reason why other existing warrants could not be obtained to achieve exactly the same result. If someone from the shop rings up and says that they have got some person—the implication is that the person is a terrorist—who is ringing them up to make unusual purchases, then there is no reason why a service warrant could not be obtained to intercept the line or that a named person warrant could not be obtained in order to deal with that. There is really no reason to have a B-party warrant where you tap the phone

run by the chemical shop owner and then all of the private conversations made between that person, their family, their doctor and many other people are also intercepted.

Dr Bibby—To come back to the balance point, one of the requirements for balancing when there are conflicts of rights or conflicts of principles is that the intrusion on the overridden right is the minimum that is necessary for the purpose. The justification which is offered for overriding privacy in this case is that it is necessary to save life. It is the only one that really makes sense. But we have a law here which is proposing to override it very substantially more than is needed for that purpose. The second standard requirement—there is nothing new about this—is that the thing is going to be effective. There is no value, no moral legitimacy, in overriding a right unless you have good reason to believe that it is going to work. But, as I said, there is no reason to believe that this is going to work. You could think of ways of getting around this legislation in five minutes once you knew it was ready.

Senator STOTT DESPOJA—Does the council have a view on the issue of legal professional privilege?

Mr Murphy—Of course it is an obvious problem. The people who are, in our view, most likely to be subject to B-party warrants are going to be people like lawyers who are in contact with people who may be suspected of a criminal offence. It may also be people like journalists, who may be following a story or may have someone contact them because there is something of interest. With regard to issues of legal professional privilege, it is one thing to say that that can be argued later in terms of the admissibility of evidence, but if you are going to provide this power then you need to provide an immunity so that anything that is not directly related to the investigation for which the warrant has been obtained needs to be expressly excluded from being used in evidence against anybody else. I am not sure that the legislation adequately deals with that.

Senator STOTT DESPOJA—Is that in addition to doing what the Law Council suggests, which is expressly stating that the schedule does not override legal professional privilege?

Mr Murphy—Absolutely. If the only purpose—and this is what is being put by the agency seeking this power—is to assist them in an investigation of a suspect, and the innocent B-party is not the focus of the investigation, then there should be no difficulty in providing the innocent B-party with immunity from prosecution for anything else that is not related to the original offence. Otherwise, if that is going to be argued against by the agencies, the inference that you can draw from that is that this is nothing more than a fishing expedition and it is about enlarging the information that you collect on the off-chance that you may find someone incriminating themselves or providing sufficient information for which the police can then go on and ultimately charge them with an offence.

Senator STOTT DESPOJA—You may have heard us discussing—so long ago!—with the Privacy Commissioner and I think with the department the issue of destruction of evidence or stored communications and that this should happen forthwith, according to the legislation. Do you think there should be stronger parameters or specifications, including a time line, on the destruction of that information?

Mr Murphy—There should be. The clearer the legislation makes it then the less scope there is for a problem later on. If it is necessary to keep information because an officer might

be engaged in some criminal activity, then there could be an exemption there where, if the chief of the organisation or somebody else needs to, they have got the power to extend that for that reason only. But there needs to be a time limit on it. You are not dealing here just with agencies that are used to interception, that have had the power for a long time. You are expanding this to all sorts of agencies that may not have the capacity to effectively comply with the requirements. If they are given a very lax provision which just says, 'Do it forthwith,' and that is then confused with other elements of the bill that seem to mean, 'Do it when you get around to it,' then you are going to find that the information is held for an extraordinarily long time—and the longer it is held the more capacity there is for it to be inadvertently leaked or misused by somebody. That is the real danger.

I might say that the breach of someone's privacy is not in that information later becoming public. Once it is obtained—the officer there is listening to someone's private conversation: somebody else knows—that is when the breach of privacy occurs. And it really does not help or comfort people to know that it might be stored for an even longer period of time.

Senator STOTT DESPOJA—I think we were trying to make that point. Thank you both.

Senator LUDWIG—There are a couple of matters that have arisen today that I think you might want to reflect on. I know you heard some of the evidence. One matter was the interception of the handset. Do you accept the evidence that they can only use it when they can uniquely identify the handset?

Mr Murphy—No, I do not accept that. It appears to me that the bill encourages them to do that but that they may still be able to obtain a warrant without having done that, because there is nothing that would expressly require them to convince the issuing authority that they had identified it.

Senator LUDWIG—I do not know if you have had an opportunity to look at the EFA submission and, in particular, what they say about B party and the additional protections that they suggest. But if you look at paragraph 12.9 of the Blunn report, the evidence was that—save one, maybe two—those protections meet the requirements under the Telecommunications (Interception) Act. What one of them turned on was the question of how you interpret section 46, about the material. I do not know whether you were here during that evidence.

Mr Murphy—I do not think so.

Senator LUDWIG—Then I might not put it to you, because it would be unfair. One of the issues of course is that B-party interceptions are a last resort. EFA argue that they are a last resort—and I am summarising because of the time available.

Mr Murphy—The legislation that is proposed does not make that expressly clear. The process of requirements—this is from memory; I do not have the report in front of me—suggests that it would be better to use other mechanisms first, and then once they have exhausted those use this, as I understand it.

CHAIR—Yes.

Mr Murphy—In my view you cannot read that to mean it is as a last resort. It does not equate. You may well have agencies obtaining B-party warrants because it is more convenient to obtain the information that way than by using a traditional warrant.

Senator LUDWIG—But if they have exhausted all practical means?

Mr Murphy—But what is the real definition of 'practical means'? It may well be just more economically efficient to go about it this way than other ways. It may be extraordinarily difficult for them to do it another way, but they may well be able to obtain the information that way. Yet this seems to allow them to simply exercise the option of a B-party warrant.

Senator LUDWIG—On the basis of practicality.

Mr Murphy—The whole point, as I say again, is that the act is there to protect people's privacy so that you are only invading someone's privacy in intercepting a phone line when there is a need to do so to further a criminal investigation. What this legislation seems to allow is another option, effectively, where it might be more practical to use a B-party warrant than it is to use another type of warrant or some other form of investigation.

Senator LUDWIG—The issue of derivative uses has also come up a number of times, and the response from Attorney-General's seems to be that they are currently available under the Telecommunications (Interception) Act and therefore, by analogy, should be available with a B-party intercept. Do you accept that proposition put by AGD?

Mr Murphy—If that is the position then there should also be no problem in amending the legislation to make it expressly clear.

Senator LUDWIG—Yes.

Mr Murphy—And that should be done to avoid any doubt.

Senator LUDWIG—Thanks.

CHAIR—I think that deals with most of our questions. I just have one about the idea of a review of the legislation after a particular period of operation.

Senator LUDWIG—Or even a sunset clause coupled with a review.

CHAIR—Yes. What would your comments be about that?

Mr Murphy—I think it would be important to have a sunset clause there so that this is not something that is used in the future, as part of everyday policing activities, for ordinary criminal investigations. We are told it is needed now because of the sophistication of criminals and terrorists; that is something that may dissipate over time. We may not have the terrorist threat that we do have currently and I think, in that context, it would be valuable to put in place a sunset clause. I think it also needs review, but there are other things that could be done that would also serve to provide the public with confidence in terms of their knowledge of the way these warrants are used. There is simply no reason, in my view, why information on security warrants is not published—for example, the number asked for and how many are granted or refused. That does not identify the individual who is the subject of the warrant and there is no real reason why that information should not be published, alongside the information on the other warrants that are requested, in the Telecommunications (Interception) Act report.

CHAIR—We discussed that today.

Mr Murphy—Even if there is some view that it might affect a current investigation, the time could be extended—instead of reporting them a couple of years later, report them five years later or something. There is really no reason why that should not be done. As I said earlier, the interception warrants are covert: the person does not know that a warrant is being used to intercept their communications until it is later used in some prosecution and it becomes public.

CHAIR—You cannot complain about what you do not know about.

Mr Murphy—You cannot complain about what you do not know about. I think it is absurd to suggest that the Ombudsman in that sense provides protection for people, because people do not know. In fact it may be an offence if they take steps to find out that there is a warrant that has been issued. But, also, there is really no reason why people should not be informed, well after the fact, that a warrant has been issued. There should be a process in place where people can apply, ask for information and say, 'Has there ever been an interception warrant in relation to me or my phone line?' Once the investigation is concluded, there is really no reason why that should not be provided to them.

Senator LUDWIG—There are two points at which you could put that in: you could either put that in at a point where any query was answered or at the point where the three months had collapsed when the material should otherwise be destroyed. So your coupled question is not only: 'Has there been an interception warrant in respect of a service or my name or MAC address or alternatively the email address?'—so you might have to be clever in the way you ask—but also: 'Has it subsequently been destroyed?'

Mr Murphy—Yes, so if you are able to ask whether it has been destroyed, it is another way that you can ensure that the agencies are performing the functions they are required to.

Senator LUDWIG—Yes.

CHAIR—Dr Bibby, Mr Murphy, thank you very much. The committee is very grateful for your extended patience this afternoon while we dealt with those matters with the agencies. We do appreciate that. We appreciate your attendance today and your submission. I also thank all of the witnesses who have given evidence to the committee today and I thank the secretariat and Hansard. We have had two intensive days of inquiry and hearings. It has been a difficult process and a long week.

Committee adjourned at 4.47 pm