



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL
AFFAIRS

Reference: Telecommunications (Interception and Access) Amendment Bill 2008

THURSDAY, 17 APRIL 2008

SYDNEY

BY AUTHORITY OF THE SENATE

INTERNET

Hansard transcripts of public hearings are made available on the internet when authorised by the committee.

The internet address is:

<http://www.aph.gov.au/hansard>

To search the parliamentary database, go to:

<http://parlinfoweb.aph.gov.au>

**SENATE STANDING COMMITTEE ON
LEGAL AND CONSTITUTIONAL AFFAIRS**

Thursday, 17 April 2008

Members: Senator Crossin (*Chair*), Senator Barnett (*Deputy Chair*), Senators Bartlett, Fisher, Hurley, Kirk, Marshall and Trood

Participating members: Senators Abetz, Adams, Allison, Bernardi, Birmingham, Mark Bishop, Boswell, Boyce, Brandis, Bob Brown, Carol Brown, Bushby, George Campbell, Chapman, Colbeck, Coonan, Cormann, Eggleston, Ellison, Fielding, Fierravanti-Wells, Fifield, Forshaw, Heffernan, Hogg, Humphries, Hurley, Hutchins, Johnston, Joyce, Kemp, Lightfoot, Lundy, Ian Macdonald, Sandy Macdonald, McEwen, McGauran, Mason, Milne, Minchin, Moore, Murray, Nash, Nettle, O'Brien, Parry, Patterson, Payne, Polley, Robert Ray, Ronaldson, Scullion, Siewert, Stephens, Sterle, Stott Despoja, Troeth, Watson, Webber and Wortley

Senators in attendance: Senators Barnett, Bartlett, Bob Brown, Hogg and Kirk

Terms of reference for the inquiry:

Telecommunications (Interception and Access) Amendment Bill 2008

WITNESSES

BIBBY, Dr Richard Martin, Convenor, Civil and Indigenous Rights Subcommittee, New South Wales Council for Civil Liberties.....	10
BLANKS, Mr Stephen, Secretary, New South Wales Council for Civil Liberties.....	10
CLAPPERTON, Mr Dale, Chair, Electronic Frontiers Australia	23
DONOVAN, Ms Helen, Senior Policy Lawyer, Law Council of Australia	16
EMERTON, Dr Patrick, Castan Centre Associate, Castan Centre for Human Rights Law, Monash University	2
KELLY, Ms Wendy, Acting Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department	38
MOULDS, Ms Sarah, Policy Lawyer, Law Council of Australia	16
SMITH, Ms Catherine, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department	38
WATERS, Mr Nigel, Board Member, Australian Privacy Foundation.....	31
WHOWELL, Mr Peter, Manager, Legislation Program, Australian Federal Police.....	38
WILSON, Mr Ian, Manager, Business and Technical Delivery, High Tech Crime Operations, Australian Federal Police.....	38

Committee met at 8.48 am

ACTING CHAIR (Senator Barnett)—I call the committee to order. This public hearing of the Senate Standing Committee on Legal and Constitutional Affairs has been convened to consider the Telecommunications (Interception and Access) Amendment Bill 2008. This bill was referred to the committee by the Senate on 19 March 2008 for report by 1 May 2008. The main purpose of the bill is to amend the Telecommunications (Interception and Access) Act 1979 to extend by 18 months the operation of the network protection provisions, which are due to sunset on 13 June 2008. The bill also contains a number of provisions that deal with device based named person warrants, and I understand that this has been a major focus of submissions. The committee has received 13 submissions for this inquiry. All of those submissions have been authorised for publication and are available on the committee's website.

I remind all witnesses that in giving evidence to the committee they are protected by parliamentary privilege. It is unlawful for anyone to threaten or disadvantage a witness on account of evidence given to a committee, and such action may be treated by the Senate as a contempt. It is also a contempt to give false or misleading evidence to a committee. 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. If a witness objects to answering a question, the witness should state the ground upon which the objection is taken and the committee will determine whether it will insist on an answer, having regard to the ground which is claimed. If the committee determines to insist on an answer, a witness may request that the answer be given in camera. Such a request may of course also be made at any other time.

[8.50 am]

EMERTON, Dr Patrick, Castan Centre Associate, Castan Centre for Human Rights Law, Monash University

Evidence was taken via teleconference—

ACTING CHAIR—Welcome. We have received your submission, No. 8. It is with the committee. Before I ask you to make a short opening statement, do you wish to make any amendments or alterations to that submission?

Dr Emerton—No.

ACTING CHAIR—Thank you. I now invite you to make that opening statement, at the conclusion of which I will invite members of the committee to ask questions.

Dr Emerton—First I would like to thank the committee for the opportunity to appear, and particularly to appear by telephone link-up—especially organising that at short notice. That is appreciated. As our submission makes clear, the concern of the Castan centre is with device based named person warrants, and in particular the amendments that the bill would make to the way those warrants operate. As stated in our submission, we take the view that the proposed amendments in respect of device based named person warrants are not merely clarificatory and that indeed what they would do is make what is currently unlawful—namely, the interception of communications via devices not identified in a warrant—lawful. I think framing it in terms of that transition from illegality to legality is important because it does emphasise that the basic presupposition on which our telecommunications interception regime operates as set out in the act, the starting point, is that interception is unlawful and that there need then to be good reasons given to depart from that assumption of illegality. The main mechanism whereby that is handled is through the issue of warrants on certain grounds. Any extension of either the grounds on which a warrant could be issued or, as in this case, the scope of interception which might occur under a warrant has to be scrutinised very carefully.

Our basic point is that currently, when one looks at the act, device based named person warrants only authorise interception of communications made via a device identified in the warrant and that, if the amendments were to be passed, it would be possible rather for interceptions to be made of any device that the named person is using or likely to use, and that would be a significant expansion of the operation of device based named person warrants.

We note in our submission, and I think the Law Council submission also makes this point quite clearly, that there are some somewhat obscure remarks in sections 16 and 60 of the act as it currently stands which do seem to suggest that devices not identified in a warrant could nevertheless be intercepted. But these kinds of somewhat obscure remarks I think have to be taken to be outweighed in the act as it currently stands by the requirements set out in sections 9A and 46A that a particular device must be identified in the warrant and only interceptions of communications made via that identified device will be lawful.

I think there are good reasons for insisting on this sort of specificity or particularity as the current regime does. Firstly, the current regime does require the privacy matter to be given consideration in respect of each device to be intercepted, because that is a matter which has to

be addressed when the requesting officer makes out the grounds to the issuing authority for the warrant. A regime which diluted that requirement and allowed the agency, once the warrant had been issued, to form its own judgement as to whether or not the interception of an unidentified device would nevertheless be permissible and consistent with privacy requirements to us seems reasonably clearly inadequate. I guess we have in mind particularly Australia's obligation under international law, particularly as a party to the International Covenant on Civil and Political Rights, that our law prohibit arbitrary interference with privacy. The current way that our law achieves that is by requiring those privacy considerations to be addressed to the issuing authority and to have that matter taken under consideration when a warrant is issued. The amendments would remove that degree of protection against arbitrary interference with privacy.

I note that the Attorney-General's Department, at page 4 of its submission, suggests that agencies, in determining whether or not to intercept a device not identified in the warrant, would have to consider and form the view that the addition of a device would meet the thresholds an issuing authority must have regard to. I am looking here at the second paragraph of page 4 of the Attorney-General's Department submission. I find that quite curious because it in fact seems to suggest that we are satisfied with the situation where an agency issues a warrant in its own favour and itself determines whether or not the threshold is met. I think that clearly is not adequate oversight and does open the door to arbitrary interferences with privacy.

I make that point also by way of segue to the second main basis of concern in our submission. We have the privacy issue and the issue of arbitrary interference with privacy. We also have a very strong concern about the accountability of agencies. Particularly in the area of security and antiterrorism policing and intelligence gathering, our submission notes a number of recent matters, particularly the judgement in the case of the prosecution of Izhar ul-Haque and also the well-known affair involving Dr Mohamed Haneef. We note these events and suggest that these show that, in the current environment, there is a need for greater, not reduced, oversight of and accountability of agencies in the carrying out of their investigative functions. Our concern is that the proposed amendments, were they to be enacted, would, rather than strengthening oversight and scrutiny, weaken that oversight and scrutiny.

Our final point in our submission is that, were the amendments to be enacted—contrary to the view that we take in our submission—then we think it will be quite important that there be a reporting requirement relating to the number of devices intercepted pursuant to device based named persons warrants, which would be structurally quite similar to the existing reporting requirement in respect of service based named person warrants. That concludes our opening statement. Thank you.

ACTING CHAIR—Thanks very much, Dr Emerton. I appreciate your opening statement. We will now move to questions.

Senator KIRK—Thank you very much for your submission, Dr Emerton. It was very clear and easy to understand and set out the issues very well, I thought.

Dr Emerton—Thank you.

Senator KIRK—I just want to move to this issue of a person's privacy. It is raised in the Attorney-General's submission on page 3. The way they address the matter is as follows. They say that it is really for the issuing authority to consider the matter of the person's privacy and that the interception agency has to:

... satisfy the issuing authority that:

- there are no other practicable methods available at that time to identify the telecommunications services being used, or likely to be used, by the person of interest, or
- it is impracticable to intercept the service being used by the person of interest.

In other words, it is really for the issuing authority to be satisfied of those matters. I am just wondering why it is that you have difficulties with that, given that the issuing authority is an independent person hearing the evidence firsthand and making a decision in relation to that matter. Is that not adequate at that threshold level?

Dr Emerton—We have certainly got no concerns about the independence of judicial officers in their capacity of issuing warrants. I think the Law Council raised broader concerns about AAT members issuing warrants. They are well-known concerns about having people without tenure issuing warrants, but that is not in any sense an issue peculiar to this act or to these amendments, so I do not want to go into that issue. Our concern is a more focused concern, which is that currently—and I am looking at section 46A(2)(a)—the act says:

2) The matters to which the Judge or nominated AAT member must have regard are:

(a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant ...

I also accept that the issuing authority must have regard to those other matters that you set out from the Attorney-General's submission. On the issue of privacy, I focus particularly on that requirement in 46(2)(a) that the issuing authority have regard to how much the privacy of any person or persons would be likely to be interfered with by interception under the warrant. For the issuing authority to have regard to that matter, they must have information that would assist them in having regard to that matter. Currently, the information that they have is the identification of a particular device. Our concern is that, if the proposed amendments were to come into force, the act would contemplate that additional devices not identified in the warrant would themselves be subject to interception.

At the time of issuing, the issuing authority does not know what those devices are or might be and so has no basis on which to adequately address the question of whether or not the interception of those further devices would interfere with the privacy of any person or persons in an inappropriate fashion. The concern arises particularly in relation to device based warrants because when one looks, for example, at the explanatory memorandum for the 2006 bill, which introduced the device based warrants, it makes it clear that the logic of a device based warrant is that it is useful when a device is being used in respect of multiple services. Of course the device might also be used by multiple users.

So the concern in our submission is that, particularly in the case of a device based warrant, it seems quite possible that some person, not of interest to the authorities and who was not identified in the warrant, might nevertheless be using the device to make a communication on some service or other and then become subject to interception pursuant to the warrant. With

the current requirement identifying a particular device, the issuing authority is, for example, in a position to ask something about the identity of that device, other users of that device and so on to collect the information they need to make this determination about privacy. Once one has additional devices brought under the scope of the warrant after it has been issued, there is none of that independent oversight. In effect, the agency becomes responsible for determining whether or not it meets the threshold tests as set out in the Attorney-General's Department submission. The concern that we would have is that this is not really adequate to ensure that people's privacy is protected from arbitrary interference. In particular, I reiterate, we have in mind the privacy of third parties who might be using the device in question. I hope that makes some sense.

Senator KIRK—Absolutely. I appreciate your answer. Given the concerns that you have, how do you think the bill can be improved to address those concerns? In your view, is it a matter of just not extending it to these multiple devices? What if further accountability mechanisms were put into place?

Dr Emerton—I had not read the Law Council's submission before we put our submission in—I am not sure whether it was up at that stage—but I think they made the completely reasonable point that it is not objectionable at all in principle to name multiple devices in a given warrant. Currently, to intercept a new device, the agency would have to get a new warrant. If that was rolled into a process whereby, under the one warrant application and issuing process, they could identify and make the case for interception of multiple devices, I think that would be unobjectionable. That would in effect just be combining multiple processes into one process. There would be no reason to think that would interfere with the oversight and accountability in respect of each of those devices named. To the extent of clarification that a device based warrant can identify multiple devices, I think that would be unobjectionable. It is the notion that, upon its own motion the agency might introduce new devices which have not been subjected to scrutiny—that is our concern. Again, for the reasons I tried to make out in my answer to your earlier question, we think that the situation of service based and device based warrants is not strictly parallel because of the particular likelihood that a given device will be used by multiple users. Indeed, that seems to be one of the circumstances that triggers the logic of a device based warrant.

Senator KIRK—So what you are proposing would protect third parties' privacy?

Dr Emerton—At least that every device to be intercepted would have to be identified and argued in the issuing process, and then at that point the judge or nominated AAT member would have regard to the privacy issues surrounding that device. At that point, one then gets the normal protection that the act gives. Again, within the international human rights law framework, that protection in Australian law is the bulwark against the arbitrary interference with privacy. So I think the answer to your question is yes.

Senator BARTLETT—I think you have covered the issues fairly well, so I am not sure I need to ask too many more questions, but I am wondering about the other aspects of the bill, particularly the general extension of the sunset provisions that grant the exception to law enforcement agencies to monitor email communications. Do you have a problem with that?

Dr Emerton—We do not have a problem with that, primarily not through a strong view as to the details but rather, in my case, because I do not have a sufficient grasp of the technical issues involved to be able to form a strong opinion. Having looked at some of the other submissions from civil society type organisations and non-government organisations, I note that the concerns there tend to relate primarily to the question of when a permanent solution to the problem is to be found. To me, upon reading those submissions, those questions about finding a permanent solution seem sensible questions to ask, but because of a lack of familiarity with the technical details of that kind of network protection issue I am hesitant to express a definite view about it.

Having said that, when I first looked at it I did wonder about how this interacts with, for example, whistleblower protection mechanisms and so on. Again, I do not have a strong enough grasp of the legal dimensions of that problem to form a view, but to me the first question that arose was about the way that network protection can also involve them, particularly when it is scrutinising outgoing as well as incoming communications. It also has implications, for example, in the whistleblower protection area and that sort of area. But my grasp of both the legalities of that and the technicalities in general is not strong enough to give anything more than those very general comments.

ACTING CHAIR—Thank you for your comments. I think you have covered the main issues very well. I want to take you back to a question from Senator Kirk regarding the safeguards that apply for device based and service based named person warrants. I am interested in your views on if there should be any differences in the safeguards that apply to those matters. You have also raised reporting requirements in your submission, at page 7. You said that there should be the same reporting requirements for both. Can you flesh out your views on whether there should be any difference in the safeguards that apply and your views on the reporting requirements for both?

Dr Emerton—In relation to the issuing of the warrants, I think that a device based warrant raises more urgent privacy concerns than a service based warrant, because with the service based warrant the focus is upon the service being one that the person is using or likely to use. It is always the case, of course, that there might be other, innocent third parties using the same service, but I think that to some extent perhaps that concern is inevitable. But when we turn to devices it seems to become far more probable that another party may be using the same device but for a different service.

Mobile phone handsets are perhaps one possibility, with the swapping of SIM cards and so on. But I actually think that computer terminals are a far more likely possibility, where multiple users of a given computer terminal might be accessing quite different email accounts or other forms of telecommunication. When you look at those devices, and at the fact that a device is apt to be used by multiple users, all of whom are using their own service, you can see that, once one authorises interception on that device, one is opening the door to all sorts of people having their communications intercepted—people who may not have been identified in the warrant and may be of no interest to the authorities and who, therefore, under the basic policy rationale of the act, have a right to enjoy the noninterception of their communications. So it is that difference, in terms of picking up third parties, that obtains between device based and service based warrants. That then argues strongly that, in the case of device based

warrants, each device to be intercepted should be identified in the warrant so that the issue of privacy and the issue of third parties who might use the device can then be resolved at the point of issuing.

ACTING CHAIR—And you think that is an omission in the bill?

Dr Emerton—I think that is an omission in the bill. Currently, the act as it stands seems to contemplate the warrant identifying a single device. As the Law Council say in their submission, I cannot see any objection to the warrant identifying multiple devices. But the bill as it stands seems to contemplate that the warrant will identify certain devices, to the extent that the agency knows, but would then permit the agency to add on further devices without external scrutiny if it forms the view that these devices are ones that the person is likely to use. And it is that ability, to add on devices without having to go back through the warrant issuing process, that is our concern. Our concern is for privacy and also for agency integrity and accountability.

ACTING CHAIR—Sure. So how do we get around that? And how do you implement the appropriate safeguards to address those concerns? That is what I am interested in.

Dr Emerton—I have not actually looked to see exactly what the drafting amendments would be. But, for example, I am looking at section 46A(1)(d)(ii) which talks about:

(ii) communications made by means of a particular telecommunications device that a person is using, or is likely to use ...

That, for example, could be amended to read, 'by means of one or more particular telecommunications devices that a person is using or is likely to use'. Then at subsection (3) of the same section it says:

(3) The Judge or nominated AAT member must not issue a warrant that authorises interception of communications made by means of a telecommunications device identified in the warrant ...

Again, that could be amended to read: 'by means of one or more telecommunications devices that are identified in the warrant'. So, in effect, you could, in the act as it currently stands, change the singular to the plural, to make it clear that a single warrant can, if the agency desires, identify multiple devices, and then it can argue out the privacy question in front of the issuing authority, if the issuing authority thinks that it is a concern. I think that amendment could be quite easily made and it would not then give rise to the concerns we have. On that point, one would also have to look at those subsections of sections 16 and 60 which do, at the moment, generate a somewhat obscure suggestion that perhaps the agency, of its own motion, can add devices. And I would think, for the sake of clarity, that those particular provisions could be repealed, because, at the moment, they just introduce unhelpful ambiguity. On the safeguards issue, that would be my answer.

On the reporting issue: at the moment there is a requirement—I think it is under the relevant parts of section 100—that, with a service based warrant, the annual report on warrants issued identify the number of those sorts of warrants which allowed interception of, I think, up to three or five or 10 services, and also the total number of services intercepted. So one can get a sense from that of how wide ranging these service interception warrants are. And I think, if device based warrants were to allow multiple devices to be intercepted, it would be helpful to have a comparable reporting requirement which would indicate, again,

roughly how many warrants allowed interception of what number of different devices. So then, in terms of public review and information, and policy development in the future, we could have a sense of how wide ranging these device based warrants are.

ACTING CHAIR—I have read the comments on page 7 of your submission about the reporting requirements. The bill is currently vacant in terms of device based warrant reporting?

Dr Emerton—That is right.

ACTING CHAIR—Would you recommend inserting a further provision in that regard?

Dr Emerton—Yes, we would be recommending inserting a provision. Having been written in a short time, our submission does not draft what the provision might look like, but in structure it would be extremely similar to those current provisions in paragraphs (eb) and (ec) of subsections (1) and (2) of section 100. I think that identical provisions that talk about devices rather than services would structurally do the job nicely for device based warrants if they were to permit interception of multiple devices.

ACTING CHAIR—Sure. Have you had a look at the views of the Australian Federal Police or the Attorney-General's Department on this matter? As a devil's advocate, can you see where they are coming from?

Dr Emerton—I have had a look at both those submissions. I hope I have made clear what my response is to the Attorney-General's Department submission in particular. I am speaking fairly consistently here with the Law Council's submission. The suggestion in their submission that you satisfy the privacy requirement through the initial issuing process is not adequate. If the bill permits an agency, of its own motion, to add devices after the point of scrutiny, at that point it is no argument to say, 'We had earlier scrutiny,' because that earlier scrutiny did not scrutinise the matter which is of concern, namely, the subsequent addition of devices. My memory of the AFP submission is that it primarily addresses the technical question of the identification of particular devices. That technical question is something on which I have no particular expertise, so I am not able to address that.

I reiterate the point we make about agency accountability and efficiency. I think some recent events show that it can be in agencies' own interests to be subjected to a degree of scrutiny and external oversight, because it does ensure that their internal processes and standards do not become too lax or inefficient. As we have seen in certain matters, that can then lead to an undermining of their very own operations of effective investigation and, in the case of the AFP, often leading to effective prosecution. For example, I think it would be in the AFP's own interests that it have a structure of accountability where, if it were to add on additional devices, it would have to justify them to an issuing authority. That would ensure that it would not find itself getting in the sort of trouble down the track that has happened in some of these high-profile prosecutions.

ACTING CHAIR—Dr Emerton, thanks for that. The committee always welcomes any further input or suggestions you might have on improving legislation. We would welcome any feedback that you might have on improving the bill. In any event, we thank you very much for your evidence today.

Dr Emerton—Thank you very much for the chance to appear.

[9.18 am]

BIBBY, Dr Richard Martin, Convenor, Civil and Indigenous Rights Subcommittee, New South Wales Council for Civil Liberties

BLANKS, Mr Stephen, Secretary, New South Wales Council for Civil Liberties

ACTING CHAIR—Good morning and welcome. Thank you for appearing. The New South Wales Council for Civil Liberties has lodged submission No. 2 with the committee. Before I ask you to make a short opening statement, do you wish to make any amendments or alterations to your submission?

Mr Blanks—No.

ACTING CHAIR—I now invite you to make a short opening statement, after which we will pass to members of the committee to ask questions.

Mr Blanks—Thank you, Senator Barnett, and thank you for the opportunity afforded us to appear before the committee this morning. By way of opening comments, I would like to suggest that the committee consider how the passage of this bill might be affected if Australia adopted a charter of human rights, such as the type of charter that has been adopted in the ACT and in Victoria. Both the ACT and the Victorian acts, in sections 13 and 12 respectively, enshrine a right to privacy: that communications be immune from unlawful or arbitrary interference. Those rights are based on article 17 of the International Covenant on Civil and Political Rights. One would find that this committee would have before it a statement of compatibility, prepared by the minister introducing this bill, as to the compatibility or non-compatibility of the provisions of the bill with that privacy right.

In our opinion, that would produce an enormous benefit by highlighting two things. Firstly, the provision as it is drafted for device based warrants does represent an arbitrary interference with the right of privacy in contravention of the privacy right. Secondly, it would provide a discussion for the committee of all the international jurisprudence which has developed in relation to exactly this issue. Instead of Australia having to reinvent the wheel in considering how to do its covert surveillance regime, you would see instantly the large number of cases that have developed, particularly in Europe, which compare the European regimes—and there are many of them—with the privacy right in the ICCPR or the European convention. You would see that the arguments against arbitrary interference are rule-of-law arguments. These are conservative arguments, not radical arguments. They are arguments against arbitrariness. What is arbitrary about this amendment is that, having obtained a warrant, the relevant agency has the freedom of operation to apply it to any device without further independent review. That would plainly fail the arbitrariness test. That is what I wish to say by way of opening.

ACTING CHAIR—Thank you.

Dr Bibby—I have three points to make and they are all related to the submission by the Attorney-General's Department and points made in the explanatory memorandum to the bill. Firstly, it is not enough to protect privacy by restricting what can be done with information after it has been obtained. Consider a parallel with a peeping Tom. It is true that a peeping Tom invades privacy if he talks about what he has seen. He invades privacy and causes harm

by the mere knowledge that he is around and may be looking at what you are doing. But the principal invasion comes from the actual peeping itself, from actually watching what people are doing in private. Similarly, it is not enough to say, as the department appears to be saying, that you can protect privacy adequately by restricting what the police or the other investigatory agencies can do with the information after they have got it. They also cause harm by peoples' knowledge that they perhaps are being listened to or that their email or other communications are being read. But they invade privacy principally by the very act of listening itself. Any extension of police powers or of the powers of the agencies is a significant extension and a significant invasion of privacy. The police, after all, are known to break the law.

The original amendments—which were supposed to protect privacy—were made to the act because the police had a practice of breaking the law. It is on record that the Commissioner of Police in New South Wales fostered a policy, a practice, of police breaking the law by listening to telephone conversations. There is a comment in the Castan centre's material which is also relevant to us, which I will not repeat.

Secondly, it is quite clear that there was no intention in previous amendments that device based warrants should be able to be extended without any reference back to the person who gave the warrant, the issuer. It is a change which requires 12 changes in the act and changes to six of its clauses. Such a change is not merely carrying out the intention of an original amendment. Any suggestion that it is is disingenuous.

Thirdly—and contrary to the department's and the police's suggestion—this is no mere trivial change. It involves a substantial increase in the invasion of privacy of innocent third parties whose intimate conversations, medical details, youthful indiscretions, business plans and many other things that they have reason to keep private will be listened to. It is not trivial at all. We think that the proposed change should be rejected in toto. If there is an urgent matter which needs to be dealt with, it is only the sunset clause. That is all that should be left in this bill by the time it leaves the parliament.

The police will go on asking for extra powers. They will ask for them when they have no case to make at all, as they did with B-party warrants. We did not get a serious case until we got the replies on notice from the Attorney-General's Department in that matter, so no-one had the opportunity to question them. They have made no serious case for this. The police will always ask for extra powers and governments are going to be reluctant to refuse them. The only body which has a chance of doing it and getting away with it is the parliament.

ACTING CHAIR—Thank you. I will open the batting, as it were. In terms of the 18-month extension, what are your views?

Mr Blanks—We have no objection to that extension.

Dr Bibby—We have some queries about the length of it but no substantial queries.

ACTING CHAIR—What are the queries?

Dr Bibby—It just seems a long time. They have already had 18 months.

ACTING CHAIR—You have a similar view to that of the Castan Centre for Human Rights Law, whose view was expressed by Dr Emerton, with respect to the devices warrant issue?

Mr Blanks—Yes. I think Dr Emerton and the centre's submission correctly identify that this as an issue: the bill engages with article 17 of the ICCPR, and we take that one step further to encourage the committee to get into understanding what that engagement actually involves.

ACTING CHAIR—Sure. What advice do you have to the committee on further safeguards with respect to device based warrants?

Mr Blanks—We would adopt and agree with Dr Emerton's statement that there is no objection to multiple devices being nominated in a warrant. But where a warrant nominates a device and the police, or any agency, identify another device that they want to intercept, there should be a requirement to go back and obtain a further warrant. It seems to us that that would not be a significant additional burden. The AFP, in their submission, say they have to do the same amount of work to identify the additional devices, so why should the one additional step of having to obtain a fresh authority from a judicial officer, or an AAT member, be omitted?

ACTING CHAIR—Can I be a devil's advocate. In their submission, the Attorney-General's Department say that it would add further red tape and requirements in terms of time and identifying the device. They highlight the high number of devices that it may apply to and that it could complicate things. What do you say to that?

Mr Blanks—Undoubtedly, it will add another level of review of agency conduct and the question is whether that additional level of review is appropriate. The answer to that is if Australia wants to conform to international human rights standards then that additional review step is appropriate. Also, it is good practice. Why should an agency be reluctant to subject itself to independent oversight in a matter such as this where it is infringing very important rights?

Another matter is that, because the risk of interception of communications of people who are not suspects in any investigation is so greatly heightened by this sort of approach to interception, there should be introduced into the regime some provision for notice, after some appropriate period, to innocent people whose communications have been intercepted so they have an opportunity to review the lawfulness of the interception. That is something which is nowhere in the Australian telecommunications regime. The Europeans are now grappling with that. Rule-of-law considerations say that is appropriate.

ACTING CHAIR—Just on that point, you referred to international standards. Firstly, do you have any examples where legislative initiatives have been implemented in Europe, the UK or elsewhere? Secondly, with respect to your comment on international standards and device based warrants, do you have any international examples that you could point us to where this legislative safeguard has been implemented?

Mr Blanks—The most recent consideration of a national telecommunications interception regime that I have been able to find is in the European Court of Human Rights in June 2007 in relation to legislation in Bulgaria. The court concluded that the Bulgarian regime, for a variety of reasons, failed to protect the right to privacy in the way that was expected under the

European Convention on Human Rights. The protection under the European convention is essentially the same as the ICCPR protection, the ACT protection and the Victorian protection. In that judgement—it is a legal judgement—there is reference to a few other cases over the last 20 years or so where the court has been developing a body of jurisprudence, where they detail the rule-of-law requirements, emphasising that rule of law is not just about appearance and is not just a legislative authority but it is also an assessment of the quality of the law, whether the law in substance protects against arbitrary interferences.

ACTING CHAIR—You would support the recommendations regarding reporting requirements that device based named person warrants be reported?

Mr Blanks—Yes.

Senator BARTLETT—I think you have covered the core of the concerns. It is a pretty serious issue but fairly straightforward in terms of that aspect of it. I will take this opportunity to ask you a couple of questions about the broader context of interceptions at the moment. Your submission details some of the statistics. These indicate that, on a per capita basis, Australians are 23 per cent more likely to be bugged than people from the US, which I expect most people would be surprised by. I guess this is an area you monitor a fair bit, the current usage of the powers and how reasonably they are being used?

Mr Blanks—To the extent that we can get hold of statistics from the US and other jurisdictions, we do look at them, yes.

Senator BARTLETT—You also detail in your submission the purposes that are used to justify the various warrants that are issued. As you would know, in recent days we have heard talk about possible expansion of powers of interception in workplaces. I appreciate you have to focus on civil liberties, but do you think there is a justification, whether it is terrorism or other crime, to do the level of monitoring that is occurring?

Mr Blanks—Well I certainly do not see any evidence being put before this committee to justify in any objective way the need for additional powers, although I do note that the ASIO submission appears to be entirely confidential. There is no part of it that is available, so I do not know what is in that. There does not seem to be any particular discussion going on in the public arena which points to a requirement for greater and more arbitrary interference with telecommunications.

Senator BARTLETT—Accepting the limitations on access to information, do you have concerns about the specifics of how the existing powers have been used or about breaches with regard to security of the information beyond just the total number of warrants being issued?

Dr Bibby—We do not know of many cases. We would prefer to take that one on notice to see what our members might know.

Mr Blanks—I will make one comment about it. We do, from time to time, get communications from members of the public who think that their telecommunications have been intercepted and wonder what they can do to find out. Of course the obligation on their telecommunications carrier is to make no comment. There is the opportunity to go to the Telecommunications Industry Ombudsman and ask there, but generally speaking you do not

get any meaningful response from there. It goes back to the comment that I made earlier—that is, that people whose telecommunications are intercepted but who are not suspects in any investigation or the investigation which led to the interception has concluded should be provided notice so that there is some means of testing whether or not interceptions have been lawfully conducted and reasonably conducted. At the moment the statistics that we have are the only statistics, the only information that is really available. As you see, 50 per cent of interception warrants seem to lead to an arrest. Now, it is a matter of judgement as to whether that figure is acceptable or not.

Senator KIRK—Thank you for your submission, gentlemen. I am interested in the second paragraph on page 2 where you talk about the fact that here in Australia 93 per cent of warrants are issued by nonjudges—and I assume you mean AAT members—and you point out the obvious fact that these members do not have judicial tenure, unlike chapter 3 judges. You then state:

It is a reasonable conclusion that interceptions in Australia are being authorised and undertaken for inadequate reason, and without regard for the privacy of those affected.

I wonder how you draw that conclusion. Can you also comment on the need for an independent observer and participant in warrant hearings, along the lines of what happens in Queensland? I am just asking you to elaborate somewhat more on the points that you make there.

Mr Blanks—I think that, if you asked any investigator in any of the agencies to compare their experiences when they approach Supreme Court judges for warrants with their experiences when they approach AAT members for warrants, they would tell you that there is a significant difference in the level of scrutiny that is applied to the application and the level of consideration that is given to the interference with privacy rights. One concludes from that, given the very high proportion of warrants that are issued by the AAT compared to by Supreme Court judges, that there are some warrants being put through which may not survive the scrutiny of a judge. That is a matter of serious concern.

Senator KIRK—So you are not suggesting any change at this point to that system?

Mr Blanks—If we had an opportunity to suggest a change to that system, we would. This bill of course does not deal with that. I suppose the act could be amended to make that change.

Dr Bibby—Indeed, we have repeatedly asked for that in submissions to earlier amendment bills.

Senator KIRK—As you say, it is not really relevant to this bill. I was just interested in your view on that. Also, I notice in your last paragraph that you set out some interesting statistics in relation to the issuing of warrants and the types of subject matters for which they were issued. As I understand your conclusion there, you are saying that the committee should take this into account when we are giving consideration to whether these powers ought to be extended in the manner proposed by the bill. I wonder if you could elaborate a little bit for us on that matter.

Dr Bibby—The statistics themselves come from the annual report as presented to parliament. We think they speak for themselves, but we would want to discourage anybody

from thinking that this bill is about terrorism or about cases where life is in danger. This is a bill that is principally about drug dealing and other lesser offences. It is important to bear that in mind when you consider what sorts of changes are justified.

Senator KIRK—You obviously object to the bill, but you would not have an objection if there were to be a further process of scrutiny if and when additional devices were to be added to the warrant—if there were to be a new scrutiny process introduced whenever there were to be further devices added—is that right? Is that your primary objection?

Dr Bibby—‘Primary objection’ would be a bit rich because we object to a great many things about the process and have put many changes like the introduction of a public interest monitor and so on. We would like to see it all governed by a charter of human rights and so on. Yes, we would still have objections, but the situation that is here at present would not be made significantly worse if all the multiple devices were identified in the warrant process, because at least then the person issuing the warrant—the judge, as we would hope, or the AAT member, as it may be—would know the extent to which privacy was being invaded and would actually be able to do what the act requires them to do: to take that into account before issuing a warrant.

Senator KIRK—And if there were to be an additional device identified down the line by the agency, provided that were to be brought before an AAT member again, then you would be more or less satisfied with the fact that there had been adequate scrutiny—is that fair to say?

Dr Bibby—With the same provisos. It would not make the situation any worse; they would just be asking for a fresh warrant.

ACTING CHAIR—Thank you very much for your submission today. It is appreciated.

Dr Bibby—I would like to make a final comment. It is to the point about overseas countries which have introduced arrangements for people who have had their communications intercepted to be told later on. There is a domestic example. Under New South Wales law—I think it is when a house has been entered and searched without the owner knowing about it, but I can check that if you are interested—after two years, unless a Supreme Court judge orders otherwise and unless there has been a subsequent prosecution, the owner of the premises and the principal occupier have to be told that their premises have been invaded. We would like to see a similar thing with interceptions of telecommunications.

ACTING CHAIR—Thank you.

[9.47 am]

DONOVAN, Ms Helen, Senior Policy Lawyer, Law Council of Australia

MOULDS, Ms Sarah, Policy Lawyer, Law Council of Australia

ACTING CHAIR—I welcome the Law Council of Australia to our hearing. Thank you very much for being here. We have received your submission and it has been lodged with the committee. Do you wish to make any amendments or alterations to it at this time?

Ms Donovan—No.

ACTING CHAIR—I now invite you to make a short opening statement after which we will move to questions.

Ms Donovan—The Law Council is grateful to have this opportunity to appear before the committee today. We were concerned that the bill might pass through parliament without being subjected to the sort of attention and scrutiny it deserves, so this inquiry by the committee is most welcome. The Law Council's submission is primarily concerned with the proposed amendments to the provisions regarding device based named person warrants. The Law Council, like the previous submitters, does not object per se to more than one device being named and included in a single warrant. Our objection is to the addition of devices to the warrant after its issue and without the express authorisation of the issuing officer.

It seems police, government, privacy commissioner, civil liberty groups—everyone—agree that a warrant should be required to undertake interception of this kind. That reflects an acknowledgement that these powers may, by their very nature, result inadvertently or otherwise in an unwarranted invasion of privacy. The warrant process is supposed to safeguard against this but it cannot fulfil that purpose unless the issuer of the warrant is required to be satisfied of, we would say, at least four things.

Firstly, that the person whose telecommunications are going to be intercepted is a legitimate target of suspicion according to the test set out in the legislation. Secondly, that intercepting that person's telecommunications is likely to yield useful information for the investigation. Thirdly, that any telecommunications device covered by the warrant is used or is likely to be used by the target suspect. Fourthly, that any telecommunications device covered by the warrant can be uniquely identified such that telecommunications made using that device can be isolated and intercepted with precision.

The amendments that are proposed here make steps three and four of that inquiry process impossible, and that significantly undermines the purpose served by obtaining a warrant in the first place. The amendments remove any onus on police or ASIO to establish to the satisfaction of an outsider that there is both a sufficient and a demonstrable link between the telecommunications device targeted and the suspect, or to establish that they have the capacity to home in on telecommunications made via that device and no other. Given what we have been told in the past about the reliability and the accuracy of device based interception, this should be of some concern.

Part of the department's response to such concerns, which was alluded to earlier by Senator Kirk, is that there is an overarching obligation on the issuing authority to consider, before

issuing a warrant, the impact interception will have on the privacy of the person using the device. But our very point is that this is not something which can be meaningfully considered in the abstract without knowing precisely what device is going to be the subject of interception. Another part of the department's response to these concerns is to point to the reporting and oversight mechanisms, which monitor the use of powers after the issue of a warrant. Obviously these sorts of safeguards are very important, but they are not a substitute for a rigorous warrant regime. Anyone who reads the annual reports, for example, would see they are concerned with accountability on a much more general level and are not properly designed to safeguard against individual rights in each and every case.

In closing, I would just make one further point. These amendments have been billed as technical in nature, and more recently the department has said that essentially the amendments correct a drafting problem with a bill that introduced device based interception in 2006 and do no more than give effect to parliament's intention when it passed that bill two years ago. Given the current wording of the act and the sorts of statements that were made by the government at the time the 2006 bill was passed, the Law Council does not think that those arguments are sustainable. These are not technical amendments; they did not give effect to parliament's 2006 intent. The amendments extend an existing power, and that should be transparently acknowledged and the amendment should be evaluated in that light.

ACTING CHAIR—Do you have a response to the 18-month extension?

Ms Donovan—No, we do not have any objection to that per se. We are not in a position to say what its impact is at this point in time. I note that one submission, which I think was from the Commonwealth Office of the Privacy Commissioner, said that perhaps the exemption does not need to be continued in quite such blanket terms and there may be ways that it could be narrowed to identify which people within agencies covered are able to conduct interceptions and what use may be made of information which is obtained pursuant to that exemption. But I think they are probably in a better position to comment in that respect.

ACTING CHAIR—And, just to get clarity on your response to the minister's second reading speech saying that these technical amendments are merely to clarify the law, your response to that is that that is not accurate, that is wrong. Is that correct?

Ms Donovan—They definitely do much more than clarify the law; they are changing the nature of the warrant provision. At the moment it is very clear that the warrant must state the particular device which can be intercepted pursuant to that warrant, and these amendments would mean that devices could be added to the warrant after the warrant was issued. That is quite a different power, clearly.

ACTING CHAIR—Have you perused the Australian Federal Police submission and the Attorney-General's Department submission? Being a devil's advocate, looking at it from their perspective, can you understand that this would add a further layer of what they may say is red tape, certainly time? And they would say it is difficult to clearly identify the devices that may be subject to such a warrant. What do you say to those arguments?

Ms Donovan—I think there are a few responses to those arguments. Firstly, they are often put in terms of 'criminals are using 80 mobile phones and 80 SIM cards and cycling through them very quickly'. That may well be true, but if we look at the reporting which has gone

with the service based named person warrants to date, we see that the majority of those warrants have only been used to intercept between two and five services. The 80 mobile phones and 80 SIM cards example may well be the exceptional example, and I do not think we should necessarily be legislating for that exception. But the department or the police can respond further to that.

Secondly, I would say that whether the agency has to go internally or externally to add another device to the warrant we would expect—and I think we would be concerned if it were otherwise—that whoever is in charge of the operation would have to make that case to somebody and would have to document to somebody why they want to add a device to the warrant and what information they have for that purpose. I think the fact that that process has to be external rather than internal does not really add that much more red tape, and it is certainly preferable that it be external.

ACTING CHAIR—What are your views on the merit of the reporting requirements as outlined by Dr Emerton? I am not sure if you had a chance to listen to his comments or have read the Castan Centre for Human Rights Law submission.

Ms Donovan—I did. I think Dr Emerton's submissions were made on the basis that if the legislation is not amended then certainly there should be a requirement that the number of devices ultimately intercepted under any particular warrant should be listed, and we would certainly agree with that.

ACTING CHAIR—And that is not included in the bill?

Ms Donovan—No, that is not included in the bill. I think, as it is, the number of services intercepted has to be reported upon. I may be incorrect on this—the department can clarify—but as it stands if, say, five services were intercepted on the basis of a particular device being intercepted then that would have to be recorded. However, you could not tell how many devices had been the subject of interception.

ACTING CHAIR—Have you considered possible amendments to the bill to fix the particular concern about the safeguards applying to the device based warrants?

Ms Donovan—No, because originally our position was that those amendments ought to be rejected. As we have stated, we do not object to the bill being amended in an alternative way—which would be to allow multiple devices to be covered under a single warrant provided they are named at the time.

ACTING CHAIR—That is my point—have you considered an actual drafting?

Ms Donovan—No, we have not, but we could provide a formulation to give effect to that.

ACTING CHAIR—The committee would welcome any input in that regard, particularly in light of the time frame that we face in terms of (1) delivering our report and (2) this legislation being considered swiftly.

Ms Donovan—We will certainly take that on notice and get back to you as quickly as possible.

ACTING CHAIR—Thank you so much.

Senator KIRK—Thank you very much for your submission. I found it very comprehensive and most useful. You make a comment on page 9 of your submission. From the way I read it, you say that the department, when being questioned in relation to the 2006 bill, appeared to make it clear that the ‘warrants will only be issued’ when a ‘unique identifying number’—that is, a unique, distinct device—could be identified. You go on to say that the undertaking by the department ‘demonstrates a clear legislative intent that the particular device from which communications are to be intercepted would have to be identified at the time the warrant was issued’. You conclude from that that it was intended that the device be identified at the time and that subsequent devices identified would not be added onto the warrant. You then go on to say that ‘this should not be used’ in order to loosen the regime to allow subsequent devices to be added on. Are you suggesting that there are some unintended consequences in this legislation, or do you think that the legislative intent is quite clear that there be these multiple devices?

Ms Donovan—With this bill, I think the legislative intent is very clear that there would be the capacity to add additional devices after the warrant is issued. I think that the legislative intent of the 2006 act was very clear also, but if you look at sections 16(1A) and 60(4A)(d)—the latter of which deals with notification to the telecommunications carrier of the addition of an extra service or device to a warrant—they both seem to envisage that a device could be added. But, at the same time, those sections also reiterate sections 9A and 46A in talking about a particular device named in the warrant. I think it is a drafting error and our concern is that those sections, which we would describe as subsidiary sections, are now being used to attribute to the 2006 parliament an intent which they clearly did not have and which goes against the undertaking that was given by the department in a response to this committee’s report at that time.

I do not know whether the department presses that issue and it is probably not important because, as we said, the legislative intent of this bill is clear. It is just that we think that these sorts of debate ought to be had on a very open basis. They should say, ‘This is the introduction of a new power. We think it is justified; this is why’, rather than introducing it as somehow just fixing some minor problems that do not have any real impact on the regime as it is.

Senator KIRK—I wanted to ask you another question as well. Clearly this is part of an ongoing process. The sunset clause is being extended for 18 months in order to allow a more comprehensive review to be undertaken as to how these matters ought to be dealt with. Has the Law Council given any consideration to the broader question of the Blunn report and a long-term solution to dealing with these matters?

Ms Donovan—On the network protection issue, no, we have not given any further thought to that. We understood, and the bill presented this as well, that those network protection provisions were in place for certain agencies and that they did not necessarily need to be that broad or worded in that way but that they would be refined and something more precise but still workable for those agencies would be introduced. The media in the past few days has suggested that the extension of this sunset clause is not just to allow the refinement of this existing exception but, in fact, to allow the expansion of that exemption to cover not just government agencies but perhaps private employers as well. Obviously, that is of some

concern, but we will look at the proposals when they are available and evaluate them accordingly.

Senator KIRK—Sorry. It is difficult for you to comment in the absence of anything that you can actually examine, isn't it?

Ms Donovan—In the abstract, yes. It is not our position to just resist things per se.

Senator KIRK—Of course, yes.

Senator BARTLETT—I just want to touch on that issue. I realise you have to assess future changes on their merits but, given what the existing sunset clause allows, do you think there is any possibility that private sector organisations are currently inadvertently breaching the law as it stands?

Ms Donovan—I am not really in a position to answer that question. I think that that is certainly what the discussion has revealed in the last few days. The fact that such an exemption might be necessary has perhaps alerted people to the fact that the current position is not that clear and what they thought was lawful is perhaps not lawful. I cannot offer a more detailed answer.

Senator BARTLETT—You have submitted that devices may be added to a warrant:

... notwithstanding the fact that the issuer of the warrant has given no consideration as to whether there is sufficient available evidence to link the named person to those additional targeted devices or whether there is sufficient available information to uniquely identify those devices ...

What is the practical effect of this? Is that likely to enable a carte blanche expansion without proper scrutiny?

Ms Donovan—The fear certainly is that—

Senator BARTLETT—There is no legislative protection against that.

Ms Donovan—Yes, there is no legislative protection against it. There is no external scrutiny. While internal procedures might and probably would be developed and more often complied with than not, we as outsiders and the parliament cannot be satisfied that those protections are in place and are uniformly observed.

Senator BARTLETT—The government has asserted that the amendments will bring the device based warrant regime into line with the service based warrant regime. Do you have a response to that assertion?

Ms Donovan—I think that ignores the fundamental difference between service based interception and device based interception. The risk of invading the privacy of third parties who are not the subject of investigation is much greater with device based warrants. That is acknowledged in the legislation itself, which continues to say that device based interception is a measure of last resort when the services cannot be identified. In fact, the department's responses point to those provisions which demonstrate that device based interception is a measure of last resort as being one of the safeguards that are available in the act. There is an inherent inconsistency in pointing to those provisions and at the same time arguing that service based and device based interception should be on the same footing. That does not even take into account the fact that in 2006—and the situation may have changed; no doubt

the police and the department can address you on this—beyond those privacy concerns there were concerns that device based interception was not as reliable and accurate because the technology was not necessarily available to ensure that each and every time a device was intercepted only that device would in fact be intercepted.

Senator BARTLETT—Are you satisfied with the threshold test of likeliness in relation to the device usage of a suspect, or would you prefer to see some sort of higher threshold?

Ms Donovan—I think that the test of likeliness is probably satisfactory at this point, although—and I think Senator Kirk alluded to this before—regardless of what tests are in place, there is perhaps room for inserting a third party, a public interest monitor, into this process so that, regardless of what the test is, it is applied in an adversarial environment where the evidence and the assertion of the agency seeking the warrant are subject to some contest. I think it is very difficult for the issuing authority to receive information and assess it critically when there is not another party to challenge the evidence that is put before them. That is probably more important at this point than changing the word ‘likely’ to ‘more likely than not’ for example.

Senator BARTLETT—Whatever the threshold is, the key thing is making sure it is properly applied.

Ms Donovan—Exactly.

Senator BARTLETT—Within reason—as long as there is some threshold.

Ms Donovan—There is a very high success rate for applications. I am not suggesting that means that the process is not being properly applied. It may be that just the fact of the external authorisation process is, in itself, enough to ensure that these are only applied for when they should be and the documentation is in order. We do not know that because this takes place ex parte in chambers and no-one is privy to it. Certainly, I think only good could come from injecting another party into that.

Senator BOB BROWN—With respect to the potential for state ministers and attorneys-general not to know that surveillance has been applied for and that surveillance of citizens is taking place, do you see that as a problem?

Ms Donovan—I did not understand your question.

Senator BOB BROWN—The concern that state agencies may be seeking warrants without the knowledge of their ministers apparently arises out of the legislation as it currently stands. The federal Attorney-General would know but not necessarily the state minister.

Ms Donovan—As a result of the changes in the reporting requirements?

Senator BOB BROWN—Yes.

Ms Donovan—I am afraid I am not in a position to comment on that. We have not looked at those in detail, but I can take it on notice.

Senator BOB BROWN—Can you give a practical example of the concern you would have about an innocent citizen potentially falling foul of an application for surveillance under the legislation as proposed?

Ms Donovan—Under the legislation as proposed, a device could be added to a telecommunications interception warrant after the issue of the warrant. That device may be, for example, a computer which can be accessed in a public place but, because the interception warrant does not only relate to a particular service that is used via that computer, anyone who uses that computer would potentially then be subject to interception. But the issuer of the warrant would never have considered where the device was located or who else used that device and therefore would never have given consideration to the privacy impact of allowing the interception of that device.

Senator BOB BROWN—In fact, in the case of a publicly used computer, it would almost certainly be the case that other users would have their information picked up in the course of the surveillance, wouldn't it?

Ms Donovan—I assume so.

ACTING CHAIR—I thank the Law Council of Australia for their submission and for being with us today.

Proceedings suspended from 10.12 am to 10.34 am

CLAPPERTON, Mr Dale, Chair, Electronic Frontiers Australia

Evidence was taken via teleconference—

ACTING CHAIR—I now welcome out next witness. We have received your submission, No. 11. Do you wish to make any amendments or alterations to that submission?

Mr Clapperton—I do not.

ACTING CHAIR—I now invite you to make a short opening statement, at the conclusion of which I will invite members of the committee to ask questions.

Mr Clapperton—Thank you. As members of the committee are probably aware, the issue of telecommunications interception has become exceptionally topical this week, with comments made by the Attorney-General over the weekend sparking a flurry of media activity concerning the issue of telecommunications interception and security in the context of providers of critical infrastructure services. This issue touches on the sunset provisions dealt with by the bill, which were not addressed in our written submission. Because they have now become topical I will briefly address this issue.

Since at least 2006 it has been known to the Commonwealth government that there is some degree of uncertainty surrounding the legal position of commonly used security technologies such as spam and virus filtering of incoming emails. It is at least arguable that this type of commonplace activity amounts to an unlawful interception of telecommunications and is therefore an offence under the provisions of the Telecommunications (Interception and Access) Act. Although in 2006—the extension of the sunset period is part of the bill currently before the committee—exemptions were put in place for organisations such as ASIO, the police and anticorruption agencies, it seems, at least on the basis of publicly available information, that nothing has happened since that stage to address the situation as it applies to other organisations.

In our view this is not a satisfactory state of affairs. Simply put, it seems now that ASIO, the police and anticorruption agencies may be able to legally filter viruses and spam from their incoming email but there is a good chance that organisations in the private sector and indeed governmental organisations not specifically provided for in the legislation may be committing an offence by doing that. It is now proposed to extend the period under which the police and security agencies enjoy this special exemption for another lengthy period of time, thereby ensuring that their activities remain lawful while leaving everybody else operating under a cloud of legal uncertainty.

It is our position that this issue should have been fixed well before now. We have heard no explanation from the Commonwealth as to why it is the case that this has not been addressed. We feel that it does now need to be addressed as a matter of urgency and not put off for another 12 or 18 months.

Turning to the issues addressed in our written submission—that is, the amendments which were characterised by the responsible minister as minor technical amendments conferring no new powers on police agencies—we take issue with that characterisation for the reasons set out in our submission. In broad terms, the amendments would almost remove the need for

scrutiny of warrant applications or at least named person device based warrant applications by the issuing authority. It would at least remove the need for each device which an organisation proposes to intercept from being named in the warrant. Essentially, once one of these named person device based warrants is issued, the organisation intercepting the telecommunications is then essentially free to decide behind closed doors and without outside scrutiny what devices are 'likely' to be used by the person named in the warrant. For the reasons given in our submission we believe it is simply an unacceptable state of affairs that agencies are able to decide on the basis of information that is not subject to outside scrutiny and indeed may not be admissible in a court of law what devices are to be the subject of intervention.

The power held by police and intelligence agencies to intercept telecommunications services and devices is one of the nuclear weapons of the police powers, as much the same way as Anton Pillar orders could be described as the nuclear weapons of civil discovery. As with Anton Pillar orders, they are extraordinary powers which are inherently susceptible to abuse. They must be subject to strong safeguards for the protection of the rights of individuals.

ACTING CHAIR—Thank you very much. I will pass to Senator Kirk for questions.

Senator KIRK—Thank you, Mr Clapperton, for your submission. I take it from reading your submission that it strongly endorses the comments and the recommendations made by the Law Council of Australia.

Mr Clapperton—That is correct. Our submission also makes some additional observations and recommendations that supplement those made by the Law Council.

Senator KIRK—As you have outlined in your opening statement? Or would you like to add anything in relation to that?

Mr Clapperton—On those areas I believe the submission speaks for itself.

Senator KIRK—We heard from the Law Council of Australia earlier today, so we are very familiar with their concerns, but is it the case that the difficulties that you have with the legislation could be overcome if it were necessary for the agency, whether it be the AFP or ASIO, to go back to the issuing authority and either seek an amendment to the original warrant or seek a further warrant in the event that an additional device is identified?

Mr Clapperton—I believe that would largely address our concerns, which were, as I outlined in my opening statement, that essentially once a warrant was issued it was then up to the discretion of the agency requesting the warrant as to what additional devices or services would be added to it once issued. This almost gives those agencies a power to rewrite the terms of the warrant, which, in our submission, is fundamentally inconsistent with the nature of independent review that the warrant-issuing process provides.

Senator KIRK—In relation to the reporting requirements, in your view should the reporting requirements for service based named person warrants and device based warrants be the same? Should they be consolidated into the one or is there a need for some distinction between the requirements for both of those different types of warrants?

Mr Clapperton—I might have to take that question on notice. Unfortunately, in the time available to us to prepare our submission we did not look in detail at reporting requirements,

although I would state broadly that, because of the nature of these powers, they do require very strong reporting obligations to mitigate the possibility of abuse by agencies holding these warrants.

Senator KIRK—Perhaps when you are looking at that you might also consider whether or not there should be any differences in the safeguards as between the two different types of warrants. That would be helpful to us.

Mr Clapperton—I would be happy to do that.

Senator KIRK—Thank you very much.

Senator BARTLETT—Could I ask you a bit more about the sunset provisions. Firstly, are you suggesting that, regarding the sunset provisions that apply to ensure law enforcement agencies are not inadvertently breaching the law, it is possible that other organisations, businesses et cetera that have virus scanning and email quarantine systems might be in technical breach of the law as it stands?

Mr Clapperton—That is our understanding of the current law. Based on consultations with the Commonwealth Attorney-General's Department it appears that they concur with us at least to the extent that the law in this area is uncertain. The position under the current law is that it is unlawful to intercept telecommunications passing over a telecommunications system without the knowledge of the person making the communication. In the case of emails received by a company or government body from outside the company or body, the person making the communication, the sender of the email, would not necessarily know that it was being intercepted. Therefore, the knowledge based exemption, if you like, from the laws in this area would not apply as it might apply in the case of interception of outgoing email, where employees could be made aware—via an internet usage policy, for example—that such interception was taking place.

There is also the issue that typically virus scanning and spam filtering of incoming emails is automatically performed by mail servers at a stage before the email is accessible to its intended recipients. The consequence of that is that, within the meaning of the Telecommunications (Interception and Access) Act, the communication is still passing over a telecommunications system at the time it is being intercepted. The consequence of the interception, combined with it still passing over a telecommunications system and lack of knowledge by the outside person, makes sending the email result in the situation where it is at least arguably unlawful to performance spam and virus filtering on those emails.

Senator BARTLETT—And that is the purpose behind the existing exemption, that there is some clause that is extended in this bill, basically to ensure that the AFP and ASIO are not in technical breach of that side of things—is that right?

Mr Clapperton—We understand that to be one of the purposes. If you refer to the provisions in the act itself that confer these exemptions on those agencies, you will see that that is not the only reason they have for those powers. For example, sections 5F(2) and 5G(2) of the act set out essentially the exemptions that apply to those agencies in that regard. Taking section 5F(2) as an example, they apply to employees, staff, officers and so forth:

... responsible for operating, protecting or maintaining the network—

but they also apply to employees, members of staff and officers who are:

... responsible for enforcement of the professional standards (however described) of the agency or authority.

It is not the sole purpose these powers are given for. The powers conferred on these agencies by the sections I have just referred to also extend to the enforcement of professional standards. The precise meaning that the agencies concerned care to give to that term would probably be a question better directed to them.

Senator BARTLETT—Going to the issue of device based warrants, does the EFA have any concerns regarding the ability of law enforcement and security agencies to uniquely identify devices that are the subject of a warrant? Do you consider it is possible to uniquely identify a telecommunications device?

Mr Clapperton—We consider that in many cases it is not possible to uniquely identify a telecommunication device by way of a supposedly unique identifier, although many types of common telecommunications devices—mobile phones, internet cards and so forth—do have identifiers which purport to be unique. In many if not most cases, those identifiers can be altered, cloned or copied, so they do not reliably provide a unique identifier. Moreover, we are given to understand that where suspects in criminal investigations, for example, might be seeking to avoid surveillance by law enforcement agencies, they might be minded to change identifiers to try to hide their tracks. In the types of situations in which these warrants might address this, there is perhaps a higher than normal chance that the identifiers may not be unique.

I note that the submission of the Attorney-General's Department to the committee's current inquiry makes reference—I am referring here to the last paragraph on page 3—to unique identifiers. They assert that those identifiers are unique and are a reliable method of uniquely identifying these devices, when that is not the case. That fact has been established by previous inquiries of this committee.

Senator BARTLETT—Would that same problem apply to computer usage, in attempting to monitor email or what websites people are accessing?

Mr Clapperton—To the extent that those activities might be carried on under a device based named person warrant, that would most definitely be the case. Changing the MAC address which is, purportedly, the unique identifier for devices on an internet based network—which is the most commonly used computer networking technology—is a fairly trivial task for anybody with a significant degree of technical expertise. So we would regard MAC addresses as particularly unsuitable as a purportedly unique identifier for computer equipment.

Senator BARTLETT—I think you suggested in your submission that the use of the word 'likely' in the phrase 'any telecommunications device that the person is likely to use' is not ideal. You suggest that the test should be that the agency be satisfied on the balance of probabilities that the person used that device. Could you just outline how you think that would establish a higher threshold. Also, do you think that is a key question or do you think the bigger issue is whether there is proper monitoring of the powers that are there?

Mr Clapperton—They are both key issues. Simply put, the use of the word ‘likely’ in these provisions and, for that matter, the other provisions of the Telecommunications (Interception and Access) Act is not sufficiently clear. As our submission states on page 2, the word ‘likely’ has been given various meanings by different courts considering different legislation at different times. Those meanings can range anywhere from the balance of probabilities, as in ‘more likely than not’ is how a layperson would probably understand the meaning of the term, to some less likely possibilities. In the context of the Trade Practices Act, for example, when looking at conduct which might be likely to have a particular effect, the standard which has been adopted by the courts is a real chance or possibility, which is significantly lower than the balance of probabilities. If the threshold for adding devices or obtaining new warrants was set that low, it would both encourage and facilitate fishing expeditions by interception agencies, not because they believed or they had evidence that a person was likely, in the sense of ‘more likely than not’, to use a particular device or service but because they thought that they might.

Senator BOB BROWN—Again, getting back to the word ‘likely’—and you have in your submission that that might mean ‘probable’ or mean something else. We do not know. It might mean more than a 50 per cent chance. Do you have a definition of the word ‘likely’ or do you think it should be taken out of the legislation and the phraseology altered?

Mr Clapperton—We would suggest that the appropriate threshold should be ‘on the balance of probabilities’—that is, it is more likely than not. Alternatively, if it is the intent of the parliament that some lesser standard should apply then that should be clearly articulated to avoid the inherent ambiguity that surrounds the term.

Senator BOB BROWN—For example, if the intelligence agency wanted to target the mobile phone of a relative or friend of a person they were tracking they would have to justify to the person issuing the warrant their reasons for targeting that other person and their device. They would have to prove beyond reasonable doubt that the suspect was going to use somebody else’s phone or computer.

Mr Clapperton—No, not beyond reasonable doubt, which is the criminal standard of proof, but on the balance of probabilities—that is, that it is more likely that they would use that device than that they would not use the device.

Senator BOB BROWN—Thank you. Do you see some way in which warrants could be limited to listening in to or surveilling that device which would minimise their ability to do so at length when it was not being used by the targeted person? In other words, when the innocent person was using the computer or the mobile phone for personal reasons or reasons which have nothing to do with a threat to national security.

Mr Clapperton—I should start this observation by prefacing it with the fact that the vast majority of telecommunications interception warrants are issued in cases that involve no threat to national security. They involve fairly pedestrian but nonetheless serious crimes in terms of attracting more than a three-year sentence. The submission of the New South Wales Council for Civil Liberties very helpfully sets out some statistics in this area. But, addressing the substance of your question, it may be possible to provide enhanced safeguards for the innocent people whose communications are caught up by the use of service based or device

based interception warrants by, for example, providing in the legislation that all communications that were not in fact made by the named person had to be discarded. It is our understanding that, under the law as it currently stands, the communications of those persons can be recorded and are only discarded if they are not really relevant to a crime which is investigated by that type of agency. I am just finding the exact paragraph. It says on page 4 of the A-G's submission:

- Intercepted material must be destroyed where it is not relevant to the permitted purposes of the agency—generally an investigation of an offence that is punishable by three years imprisonment or more.

Senator BOB BROWN—Thank you. Do you have any comment on the publicity of the last few days about the potential for employers to be asked to keep surveillance on employees?

Mr Clapperton—It is our understanding that much of the media commentary over the last couple of days does not in fact accurately reflect the intent of the Commonwealth Attorney-General's Department as it was explained to us by officers within that department—unfortunately after most of this media coverage occurred. We are given to understand that the Commonwealth Attorney-General's Department intend to clarify the legislative situation of technology such as spam and virus filtering. It is not currently their intent to confer quasi-police interception powers such as the ones whose sunset provisions are currently under discussion on agencies dealing with critical infrastructure.

EFA would support the clarification of the position of spam, virus filtering and other technologies such as firewalls and so forth. We recognise that these are necessary and appropriate tools to manage security risks. However, addressing those positions is not best served by extending the powers currently enjoyed by police and intelligence agencies to companies in the private sector dealing with critical infrastructure. That would be overkill to address the problem. We would not support the extension of the exceptions as currently drafted to organisations other than those that currently enjoy them.

Senator BOB BROWN—Thank you.

ACTING CHAIR—Mr Clapperton, I have read your submission and I have a few questions, but before I ask them can you put on the record for the committee the purpose and objectives of Electronic Frontiers Australia and a bit of background information about the organisation?

Mr Clapperton—Certainly. Electronic Frontiers Australia is a non-profit national organisation that represents internet users and the users of other communication systems that are concerned with online freedoms and rights. EFA was established in January 1994. We are a volunteer run organisation dependent on membership fees and donations for funding. We engage in advocacy and government lobbying in a number of areas that touch on online freedoms and rights, interception being one of those; other areas include intellectual property, censorship, FOI law and so forth.

ACTING CHAIR—Thank you very much. Have you had a chance to peruse the Australian Federal Police submission and the Attorney-General's Department submission? I

draw your attention to the arguments of the AFP on page 2 of their submission, where they say:

The Blunn Review identified that an interception solution was required to deal with the proliferation of SIM cards, the tendency for criminals to evade interception by rotating SIM cards through multiple hand sets and the difficulty in identifying persons who purchased pre-paid SIM cards.

They continue to talk about that, and go on to make the point:

AFP investigators determine that the device to be intercepted can be uniquely identified ...

You touched on this earlier, making the point that that can be changed rather easily. I was wondering if you could respond to the views of the AFP, in terms of cluttering up their operations and adding another layer of red tape and accountability which would prevent them from doing their job efficiently and effectively.

Mr Clapperton—There is a balance to be struck between the needs of agencies in this area to engage in lawful interception of telecommunications to further their legitimate purposes and the needs of the public to be protected from the excesses and the abuses to which those powers could conceivably be put. The AFP submission makes the point that suspects could use multiple SIM cards in one phone, and that is indeed the purpose for which the device based warrants were created: if a suspect has one phone and uses many different SIM cards in it, then only one warrant need issue naming that one device. That warrant can then be used to intercept any calls made to or from that device with any SIM card. The existence of the device based warrant addresses the concerns of the AFP in relation to ‘proliferation of SIM cards’, to use their words. We say that the balance is not struck if agencies have the ability to essentially take an eraser to a warrant after it is issued and change the significant details. That would be analogous to a magistrate issuing a search warrant that allowed the police to search not only a place which was known to be the residence of a particular suspect but any other place in which it was ‘likely’ that person might be. This really removes the need for a showing of proof and justification before an independent party that the law enforcement agency should be permitted to exercise these very intrusive powers against a particular place or device.

ACTING CHAIR—What do you say to the argument that the authorities, such as the AFP or ASIO, can with certainty identify and name the uniquely identifying device? You indicated earlier that people can change those configurations and the unique identification of the device can actually change reasonably easily. Is that your view?

Mr Clapperton—It is our understanding that, although mobile phone unique identifiers can be changed, this is nonetheless more difficult than it is for things such as MAC addresses of computers. Nonetheless, it is the recommendation of the Blunn review that warrants which permit the interception of communications based around a device are not a particularly satisfactory state of affairs unless those devices can in fact be uniquely identified. It would be our submission that at the moment they simply cannot be identified. This is perhaps a reason why the device based interception scheme should be either subject to additional safeguards or perhaps reconsidered.

ACTING CHAIR—You do not see any halfway measure in terms of safeguards—for example, the introduction of more comprehensive reporting requirements so that, once the

relevant officers have identified a certain device and they have exercised their powers accordingly, it is reported in the same way they report the services?

Mr Clapperton—The reporting obligations that attach to these warrants are really the only meaningful safeguards that exist to prevent their abuse, other than the issuing process itself. Unlike search warrants, for example, where the person who is the subject of the search warrant is obviously going to know that it has been executed, telecommunications interception by its very nature is surreptitious. The people whose communications are being intercepted do not know that it is going on and therefore they are not able to really challenge that or bring it to public scrutiny if they believe the agency is acting in excess of its powers or without sufficient evidence. The reporting obligations are really the only meaningful safeguards against misuse of these warrants. We would support moves to strengthen the reporting obligations. As to whether there might be a middle ground between preserving the operational needs of the agencies involved while protecting the rights of the people whose communications might be intercepted, we would need to look at any proposal that might be made in that area and see whether it struck an appropriate balance.

ACTING CHAIR—Sure. The submission from the Castan Centre for Human Rights Law recommended on page 7 that the bill before us be amended to ensure that the reporting requirements applied not only to the service based named person warrants but also to the device based named person warrants. Would that be something you would support?

Mr Clapperton—It would, Senator.

ACTING CHAIR—Thank you. I believe there are no further questions. Thank you for your evidence today.

Mr Clapperton—Thank you.

[11.09 am]

WATERS, Mr Nigel, Board Member, Australian Privacy Foundation

ACTING CHAIR—Welcome to our hearing today. We have received your submission, which is No. 10. It is with the committee. Do you wish to make any alterations or amendments to your submission?

Mr Waters—I have no changes, but I would like to make some opening comments.

ACTING CHAIR—We invite you to make an opening comment, after which I will invite members of the committee to ask questions.

Mr Waters—We welcome the opportunity and thank you for the invitation to appear before you. On the issue of multiple device warrants, we do not have much to add to the excellent submissions and testimony given by the other civil society NGOs and federal and state privacy commissioners. We would just like to confirm our opposition to any further relaxation of the warrant authorisation regime, which has already been weakened significantly in recent years. The need to justify successive intrusions, particularly those which can affect third-party individuals, to an independent authority is a vital safeguard against the overzealous use or the abuse of these major powers. We share the concerns of the New South Wales Council for Civil Liberties that the annual report figures illustrate a worryingly high level both of applications and of authorisations, certainly in comparison with overseas experience. That needs to be addressed separately. But those concerns about the adequacy of the level of scrutiny are not an argument for further reducing the important safeguards that those warrant authorisation processes represent. In light of the evidence given by the previous speaker, we would support a review of the definition of the term ‘likely’ in the legislation. We would support the idea of that being a balance of probabilities test.

We would like to add to our comments on the proposed extension of the sunset clause on the network monitoring exemption in light of the media coverage earlier this week of the government’s announcement of the possible extension of the exemption to private sector employers. We welcome a sensible debate about network security and the appropriate balance between security and privacy, but we are concerned that the way that ministers portrayed the issue implied that they had already decided that the relaxation of interception is necessary. It is not at all clear to us how such amendments would assist in the protection of critical infrastructure and this muddle-headed presentation of a complex issue supports our call in the context of this current bill for a better explanation by government as to the precise nature of the network monitoring difficulty and of why it is taking so long to resolve.

Such an important issue deserves a detailed and open public debate. If that is what the government intends—and we understand that their views may have been somewhat misrepresented in the media coverage—then we welcome that, but we urge the committee to seek assurances that we will not be presented in due course with a predetermined solution based on a half-baked analysis of the issue. We also take the opportunity to call for the consideration of the inadequacy of current privacy laws in relation to workplace privacy in that wider debate. Certainly any extension of monitoring or interception powers to the private sector would require, in our view, a filling of those gaps in the existing privacy coverage for

employee privacy. We also support the submission by the federal Privacy Commissioner that any short-term extension of the sunset clause to cover the existing agencies should be conditional on some additional safeguards, as the Privacy Commissioner suggests.

ACTING CHAIR—Thank you. The AFP has made a submission and we also received a submission from Victoria Police. I am not sure if you have had a chance to peruse it. In light of the changing nature of criminal activity in Australia—the new telecommunications regime, the rotating of SIM cards and, indeed, devices such as mobile phones and so on—what do you say to their concerns about having the opportunity to do their job properly, effectively and efficiently?

Mr Waters—We have no difficulty with appropriate amendments to the law to allow a response to technological changes. As the previous witness said, that is the basis of the introduction of things such as named person warrants, service warrants and device warrants. None of the safeguards that are currently in the legislation—which, in our view, this amendment seeks to weaken—prevent law enforcement agencies or intelligence agencies from doing their job. They are simply safeguards. We would argue that the marginal red tape, if you like to call it that, with the accountability mechanisms that are represented by the need to go back to issuing authorities and specify devices, services and details of changes do not in any way prevent those agencies from responding adequately to technological change.

ACTING CHAIR—I will just read to you a comment made in the Victoria Police submission:

The amendment merely extends the existing device-based named person warrant regime to authorise the interception of communications made by multiple telecommunications devices.

What do you say to that?

Mr Waters—It does that, but I think one of the submissions you have had characterises the effect of that as giving the agencies a blank cheque, partly because of the inadequate definition of ‘likely to be used’ and partly because the ability to simply add additional devices at the whim or discretion of the agencies really represents a major shift in the extent to which these powers can be used. We do not think it should be unduly burdensome for the agencies, having identified a device that they wish to intercept—which they obviously have to do in order to be able to intercept it—to take the simple administrative step of going back to an issuing authority and seeking to have that device added to the warrant or to have a new warrant issued.

ACTING CHAIR—Can I just pursue that a little further. Victoria Police say:

Sufficient privacy protections exist within the named person warrant regime and these will still be applied to applications for device-based named person warrant applications.

So the application still needs to be made to the relevant judge or AAT representative and the standard safeguards apply when making that application. What do you say to that?

Mr Waters—There are two types of privacy safeguards: those inherent in the authorisation process and the downstream safeguards. It is true that the downstream safeguards in terms of reporting and the necessity to comply with certain record-keeping requirements will still apply, but the upstream safeguards, the ones that are delivered by the authorisation process,

are in a sense negated by a multiple device based warrant because the issuing authority is simply not in a position to make the appropriate judgement about the balance of interests since they will not have any information, as we understand it, about which other individuals may be users of those devices. Therefore, the arguments about the likelihood of the suspect or the target using those is information that simply will not be made available to an issuing authority so that they can make the appropriate judgement about the balance of interests.

ACTING CHAIR—In terms of accountability measures, Victoria Police said of the issuing authority:

Examples include the requirement to revoke a warrant when the grounds for the warrant no longer exist, intercepted material must be destroyed where it is not relevant to the permitted purposes of the agency and the independent oversight of the conduct of LEA's in carrying out interception.

Mr Waters—I accept that the downstream safeguards do not change but, with respect, I simply do not think they are adequate on their own. The reality is that monitoring after the event is inevitably weaker than an authorisation process, but the resources available to the monitoring authorities, the state ombudsmen or the Inspector-General of Intelligence and Security simply do not allow them to undertake a level of scrutiny after the event that would be in any way a substitute for the authorisation process.

ACTING CHAIR—And there is not a halfway measure where you tighten the safeguards by tightening the reporting requirements? Do you think that is an option?

Mr Waters—We simply do not see why that is justified. I think the onus needs to be on the agencies to justify why they consider the authorisation process to be so onerous that it is stopping them from doing their job. To us, it smacks too much of simply being an irritating inconvenience that does not take adequate account of the good public interest reasons why those authorisation requirements are there and need to be there.

ACTING CHAIR—Do you support the recommendations by the Castan Centre for Human Rights Law, the Law Council and others to tighten the reporting requirements?

Mr Waters—We do. There were many good suggestions in those other submissions which we would support.

Senator BARTLETT—Thank you for your submission. I think you have basically answered the questions I want to ask. As I understand it, you are generally affirming the previous witnesses and the submissions they have made. One overarching aspect that niggles at me somewhat is the way this is being presented as not an expansion of powers, that it is just a technical amendment or a clarification. Given the broader ambit of your organisation and the fact that you try to monitor everything, are you aware of any sorts of evidence or debates or discussions or statements that suggest there is a need for an expansion of powers? I suppose it is one thing to expand powers, it is another thing to do it and not really say that is what you are doing. It tends to create extra suspicion. Would you recognise that there is some justification for broadening the need for law enforcement agencies to be able to do the sorts of things they want to do without extra red tape or complexity?

Mr Waters—I think there is a significant difference between extra red tape and removal of existing red tape. What we are being faced with here is an argument for removal of existing safeguards. To the extent that we support some of those requirements for additional

monitoring and supporting, yes, we are asking for some extra red tape, but we are also arguing for no diminution in the existing safeguards. In terms of the broader question, you are right: we do have a major concern about the incremental nature of the changes over the last 15 or 20 years in the interception regime. We have not opposed all of them. You have served on previous committees where we have accepted the need for certain changes to respond to both the changing nature of organised and serious crime and also the technological challenges. So we are not arguing for freezing the regime without being able to make sensible changes, but we do get irritated with the constant suggestion that every little change is just a marginal or technical amendment, which we see quite clearly as being a major weakening of the safeguards and controls over the years, without having regard to the bigger picture.

Senator BARTLETT—There are two aspects of that bigger picture that I want to ask you about briefly. One of the earlier witnesses today, I think it was the Civil Liberties Council, identified different aspects to privacy. There is the fact that if you are being monitored, it is always a breach of privacy, even if you do not know it is happening and nothing happens with the information. I guess in one sense that would be what we are assuming we are dealing with here. There is what most people would see as a much more egregious breach of privacy—that is, when the information that is gathered is misused. Do you have any comments about how we are performing with regard to that, whether there is much serious misuse of information that is gathered by law enforcement agencies or, for that matter, anybody else—private investigators?

Mr Waters—We are not in a position to keep accurate statistics on anything like that, but we would suggest that sufficient anecdotal and media coverage of irresponsible use of personal information keeps cropping up to make our concerns well founded and to put lie to the idea that you can simply trust government agencies to handle information responsibly and to keep it secure, in terms of both inadvertent leaks and losses of data or malicious abuses. Both of those are going to happen, human nature being what it is. We simply cannot afford to take the relaxed attitude of, ‘Trust us; we’re the good guys and it’ll all be safe with us.’ We have seen too many examples of that confidence being proven to be false.

Senator BARTLETT—What sorts of examples would you give? Earlier witnesses mentioned what is broadly called the Haneef incident—it was about not only Dr Haneef but also his colleague and other people.

Mr Waters—That would be one that was particularly relevant to the current issue, but, more generally, I would give the examples of the tax office and Centrelink—leakages of information and misuse by individual officers. I would also mention fairly regular, unfortunately, instances of police corruption and misuse of official information, mainly in the state police forces. These simply do not give one the confidence one would have to have to simply sweep away these safeguards in the name of efficiency. It is particularly interesting: you made the distinction between abuse of information and the more general, chilling effect of surveillance. We think one of the dangerous trends is the tendency of governments to assure us that extension of powers to monitor and surveil the activities of citizens is okay because, as they say, they will put in place the safeguards that deal with the abuse and suchlike. That, to our view, negates the important social value of privacy and freedom from surveillance as something that we actually treasure and, in most liberal democracies, value

quite highly. It simply is not good enough to say, 'If you've got nothing to hide you've got nothing to fear.' We all have the right, in our view, to basically go about our business in private unless it needs to be intruded on. The threshold tests for that intrusion need to be kept as high as possible.

Senator BARTLETT—Just one other question, on how things are going at the moment: the Council for Civil Liberties submission detailed the number of warrants being issued in Australia, which is greater in an absolute sense—quite significantly greater—than the equivalent warrants issued in the US, which perhaps we would misguidedly assume would be much more into this sort of thing. On a per capita basis it is out of the ballpark, to use an American expression. Do you have a view about whether that degree of warrant issuing is justifiable? Is that an accurate representation of the situation?

Mr Waters—The figures on the face of it do give cause for concern. We think governments, both federal and state, should be held to account for some sort of explanation as to why there is that very significant difference in the level of interception. There may be some very good reasons for it, but we have not heard them yet. It is a matter of concern that the figures do appear to be so much higher.

Senator BOB BROWN—Under the heading 'Extension of sunset clause for exemption' you say the Australian Privacy Foundation:

... suggest the Committee opposes any extension without a progress report justifying it and explaining how the issue—

of network protection—

can be resolved for all organizations, not just Commonwealth agencies.

Would you like to expand on that?

Mr Waters—It really goes to the comments that I made in my introductory remarks. We think the appropriate balance between security and privacy in the context of network monitoring is an important public interest debate which needs to be had. It does appear that, at the moment, a lot of private sector organisations are probably technically in breach of the interception legislation in their ordinary network-monitoring activities. This is an unsatisfactory situation for them to be in. It brings the law into disrepute, apart from anything else. To the extent that these laws are creating problems for intelligence agencies and law enforcement agencies at the moment, we suspect they are also likely to be a problem for a large number of private sector organisations and other government agencies that are not currently covered by the exemption. For that reason we think it is an important debate that needs to be held. The appropriate balance needs to be thrashed out. We think it is too early to make the judgement about whether it is necessary to give a wider range of agencies and a wider range of private sector organisations some sort of exemption from the interception regime. Let us have that debate without prejudging it.

Senator BOB BROWN—Are you saying that it is better to have it regulated than to just turn a blind eye to what is happening?

Mr Waters—Absolutely. If I can draw an analogy: the way the interception act applies to private sector organisations in terms of monitoring telephone calls, the law basically says that

there has to be notification and therefore all organisations should be using the sorts of recorded messages that many of us are familiar with, saying, 'This call may be monitored or recorded.' But, equally, we are all aware of many organisations that do not have those messages and yet are probably recording and monitoring. If we want the laws to be taken seriously then we need to have a debate about (a) whether they are appropriate and (b) whether they are practical, and get the balance right.

Senator BOB BROWN—Has your organisation thought of model legislation in the field?

Mr Waters—I am afraid we are not really resourced to do that. Like EFA, we are an all-volunteer organisation. We do our best from time to time to come up with positive suggestions as well as negative criticism, but we would require considerably greater resources than we have to actually draft model legislation.

Senator BOB BROWN—Just going back to the concern that has been most aired here this morning, under this legislation it would be entirely possible for an intercepting agency to be listening or monitoring communications between totally innocent and known to be innocent members of the Australian community without restriction.

Mr Waters—That would appear to be one of the potential consequences of these amendments. That is a major cause for concern and really puts the lie to the suggestion that this is simply a technical tidying up. If any concessions were made in this direction, we would certainly argue for the need for some accompanying safeguards, such as a much tighter requirement to dispose of information that was irrelevant and independent monitoring of that.

Senator BOB BROWN—And perhaps to cease monitoring information that was between persons who were—

Mr Waters—As soon as it became obvious that it was irrelevant, the monitoring should stop. We would also take the opportunity to argue—as we have done in our submission to the Law Reform Commission in their section on the telecommunications interception act—for the introduction of a public interest monitor along the lines of the Queensland model, where there is an independent officer charged with a much higher level of scrutiny of the use of these powers than the sort of downstream monitoring by the Ombudsman and the inspector-general that we have at the moment.

Senator KIRK—Thank you for your submission. I have questions in relation to the last paragraph of your submission on the reporting requirements, particularly about keeping state ministers informed of warrants. You detail that in your submission, but I wonder whether you could elaborate for the committee the concerns that you have about removing this mandatory requirement that currently exists whereby state ministers are to be informed of the warrants that are being issued? Why is it, in your view, a problem to remove that requirement?

Mr Waters—Thank for drawing attention to that problem, because I think our submission is probably the only one that deals with that issue in any depth. In our view it is an important safeguard because removing the requirement and only leaving the option of state governments choosing to opt in—which, again, human nature being what it is, is unlikely—removes an important additional safeguard, in our view, that, at least potentially, is force-feeding state governments with the information about the way in which their agencies are using interception powers. At least, it gives the opportunity for a second person to maybe spot

patterns of use that might give cause for concern. If it is all entirely left to the federal Attorney-General, you only have one watchdog. In our view, it is more important to have two watchdogs that, whilst they might not bite very often, at least occasionally might be awake.

Senator KIRK—But if the number of warrants and the nature of them is being reported on an annual basis, is that not sufficient information out there both for the state ministers and other authorities to look at in order to determine the number of warrants that are being issued? I understand that they can then only look at it retrospectively, in a sense, to see what is being done rather than contemporaneously with the issue of the warrant. I wonder whether you can comment on that?

Mr Waters—I think the reality is that, after the event, monitoring and reporting inevitably get a lower priority afforded to them. A more junior officer would probably simply flick through the reports and give them a tick; whereas if it is being done contemporaneously there is, at least, a greater chance that somebody might question whether there has been a sudden change in the pattern of use of these powers. It is just one of those additional safeguards that we would be very loath to lose.

ACTING CHAIR—Thank you, Mr Waters. I appreciate your presence with us today.

Mr Waters—Thank you.

[11.38 am]

KELLY, Ms Wendy, Acting Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department

SMITH, Ms Catherine, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department

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

WILSON, Mr Ian, Manager, Business and Technical Delivery, High Tech Crime Operations, Australian Federal Police

ACTING CHAIR—We welcome representatives from the Attorney-General's Department and from the Australian Federal Police. We have received the submission of the Attorney-General's Department as No. 4 and the submission of the Australian Federal Police as No. 12. Do you wish to make any amendments or alterations to either of those submissions?

Ms Smith—No.

Mr Whowell—No, we do not.

ACTING CHAIR—We now invite you to make a short opening statement, after which we will move to questions from members of the committee.

Ms Smith—Thank you for the opportunity for the Attorney-General's Department to appear before the committee today. I will not repeat any matters set out in our submission or in the Attorney-General's second reading speech. Instead, I would like to focus on two key points in relation to the bill. I take the opportunity to address what my department considers are the major aspects of the bills. Firstly, on the issue of network protection, I would like to clarify some misconceptions that may have arisen in regard to these provisions and recent media reporting which suggest that the government plans to introduce legislation to allow employers to intercept the email and internet communications of their employees without their consent. The bill simply maintains the status quo by extending the existing sunset provisions, thereby allowing specified government agencies to continue to protect their computer networks against electronic attacks and inappropriate use. Extending the operation of these provisions by 18 months allows time for a long-term solution to be developed that can be applied to a wider range of organisations, to provide the necessary time to effectively consult with stakeholders representing interests of privacy, critical infrastructure protection, law enforcement and security agencies. I should also clarify that the government has made no decision on the nature of a solution, nor has any legislation been drafted.

It is true that the protection of networks includes cybercrime and terrorist threats but it is also of great importance that all Australians have confidence in the security of the computer networks they use for personal communications, banking and online purchases. Proper network protection measures are essential to prevent the rapidly increasing types of e-crime associated with hacking, such as identity theft and online fraud as well as disabling attacks on networks. The main aim in developing this policy is therefore to ensure that people who are responsible for running computer networks have the tools to protect them from electronic attacks. Any longer term solution that is developed would be focused on enabling businesses

to protect their networks by scanning incoming communications traffic for viruses and other malicious software at the network firewalls.

While the act currently permits network administrators to take action once the communication has become accessible to the intended recipient, it may be too late to prevent damage at that stage. The application of the existing Commonwealth, state or territory workplace surveillance and privacy laws would not be affected by any proposal. As noted, the extension of the sunset clause for an additional 18 months will allow full consultation prior to any long-term solution being implemented.

The second important issue concerns those amendments that deal with the device based named person warrant. The rule makes technical amendments to those provisions within the existing policy framework. These amendments are essential for law enforcement national security agencies to maintain pace with technological developments. Telecommunications interception is a tool of last resort used to investigate only the most serious of offences. People who plan and carry out serious offences are well aware of interception and go to great lengths to avoid detection. In doing this, many of them take full advantage of recent rapid developments in telecommunications technology and services.

Advances in technology have created a market where multiple communications are the norm due to the low cost associated with purchasing telecommunications services. This is creating an environment whereby it is reasonably inexpensive to purchase multiple communications devices such as mobile phone handsets or laptop computers. These devices, when combined with the availability of multiple services, provide opportunities for evading detection by law enforcement agencies. In this context, legislative amendments are periodically required to ensure the operational effectiveness of the interception act, notwithstanding that the legislation is intentionally technologically neutral.

Named person warrants were introduced in 2000, reflecting at that time advances in technology that allowed people to purchase and use multiple communications services. As handsets and laptops have become more affordable and prolific, legislation was introduced in 2006 to differentiate between persons using multiple services and multiple devices. Since then we have seen these trends continuing.

To meet community expectations that serious criminal offences are investigated and prosecuted, it is important that law enforcement national security agencies can quickly adjust to this changing environment. These are the background factors driving the need for law enforcement national security agencies to intercept multiple devices under one named person warrant. While it was always intended to permit multiple devices to be intercepted under a warrant, it is necessary to clarify this in this bill. As always, though, these powers are subject to strict controls and are balanced with the privacy protections inherent in interception legislation. That concludes my introductory remarks. I am more than happy to answer any further questions.

ACTING CHAIR—With respect to the 18-month extension, to what extent had work been done in the previous period to develop a long-term solution?

Ms Smith—We have been developing a discussion paper which has not gone outside the Attorney-General's Department. What has become clear, as we look into the problem, is that

technology is moving very quickly. The types of threats to critical infrastructure are changing every single day and so we are looking at the scope of any possible solution to address the kinds of challenges that we are dealing with. We work with our critical infrastructure protection area in the department very closely and it is with them that we are actually looking at the scope of any solution.

As far as seeking the extension for 18 months, essentially we are taking into that time the fact that we have just had an election so that slowed down any development of a particular policy. Now we want to ensure that we develop a solution that allows us to consult very broadly because there are a lot of stakeholders who will be affected by any change in legislation. We want to ensure that we do not need a further extension of time, so that is why we have sought 18 months.

ACTING CHAIR—Do you feel comfortable that 18 months is adequate? Within that period you will come up with a long-term solution which will be made available to the public and the parliament?

Ms Smith—Subject to getting parliamentary access to a slot for any legislative change that would be required, we anticipate that 18 months is correct. Who would be consulted and how that consultation will be undertaken will be a matter for the Attorney-General to advise us on.

ACTING CHAIR—Sure. When will the discussion paper be completed and circulated?

Ms Smith—That is a matter for the Attorney-General. I am not aware of how that will be done.

ACTING CHAIR—But there is an internal discussion paper that is being circulated within the department.

Ms Smith—We are developing it in the department in consultation with our colleagues in critical infrastructure protection. We are both in the same division.

ACTING CHAIR—Is it completed?

Ms Smith—No, it is still in draft.

ACTING CHAIR—The issue of reporting to state ministers was raised today in the submission from the Australian Privacy Foundation. What is your response to their concerns and the issue about them opting in?

Ms Smith—I can give some background on that. Mr Tony Blunn, who undertook the review in 2005, spoke to all the states responsible for interception and talked to law enforcement agencies within those states as well as relevant Premier's and Attorney-General's departments. The view that was given to Mr Blunn was that ministers saw that, in receiving copies of warrants and then passing them on to the Attorney-General, there was not a role that they were undertaking relevant to the actual interception process. As a result, this amendment was drafted to allow copies of warrants to still be provided to ministers should they wish to receive those warrants but removing the requirement that they would be passed on to the Attorney-General.

ACTING CHAIR—But it does, would you not agree, lessen their accountability or certainly their responsibility for these activities that are being undertaken in their state or territory?

Ms Smith—No, I would not agree with that. There is the oversight requirement that ombudsmen or like agencies in the states have to undertake a review of the interception reporting requirements and accountability reports are made to each state minister by those particular oversight authorities which actually give them details of the activity that has been undertaken by the agencies within their jurisdiction. That is a much more meaningful report than receiving a copy of a warrant in a bundle with others, which is then passed on to a Commonwealth minister.

ACTING CHAIR—But you would agree that some states may opt in and some may not, so you are going to have different arrangements in different states.

Ms Smith—It is quite likely that will be the case, yes.

ACTING CHAIR—In terms of the issues that have been raised this morning, you have listened to many of the views—I am thinking in particular of the Law Council of Australia and the Castan Centre for Human Rights Law. Can we address this issue of reporting requirements? I am seeking your confirmation that the legislation before us does not include any reporting requirement with respect to device based warrants.

Ms Smith—No. The current annual reporting is on the actual services that are intercepted under warrant. The reason is that, regardless of the technology, whether it is done by device or service, it is the number of services that are intercepted that gives an indication of how many telecommunication services have been intercepted. The device is the technology by which the interception takes place. So you are quite correct. There is no additional reporting of the actual number of devices, but the number of services that are intercepted under any device will of course be in the annual report.

ACTING CHAIR—So you cannot see any merit in improving, increasing or expanding the safeguards to have a reporting requirement of the device based warrant?

Ms Smith—In my view, our reporting is among the best in the world because we actually accurately report all services that are intercepted, which does give the public a very good understanding of how many people's telephone services are intercepted. The merit of the device based warrant is not something that I can really comment on, given that I believe the information is already in the reporting.

ACTING CHAIR—Nearly all of the submissions we have heard this morning and that we have received as a committee expressed a view that the second reading speech is probably not entirely accurate in terms of clarifying the law and that rather there is an expansion of the powers with respect to device based warrants. I would like you to respond to those claims and allegations that, firstly, it is not accurate and, secondly, the reasons why the department has not taken those concerns into account.

Ms Smith—The department is of the view that it is a clarification. The nature of a named person warrant is such that it anticipates that there will be in more than one device or service intercepted. Should the government have wanted to put forward initially a device based

warrant then it would have been equivalent to a service based warrant, where there is one identified device or one identified service. When the named person warrant regime was brought in 2000, it identified that the criminal elements that were out there were using multiple services that were not necessarily possible to identify at the time a warrant was obtained because, in the period of 90 days that a warrant is in existence, the likelihood was that people would swap their SIM cards or their devices. We have anecdotal evidence that it is quite common for people to regularly throw their handsets in the bin and go and buy another one as soon as they think that they might be detected. The reason that a named person warrant device was developed was to deal with that particular challenge for law enforcement.

Although I was unfortunately not involved in the original 2006 bill, my understanding is that there were drafting errors in it. There were correct provisions, such as section 16 and section 60(4)(a), that acknowledged that it was to be multiple devices. However, the other provisions were in fact inaccurate and, once the legislation had passed, did not allow for the original policy intention for various devices to be added to a warrant.

ACTING CHAIR—Firstly, have you given any consideration to the issues of the secondary use of the data or information that becomes available during these investigations? Secondly, can you advise the committee on what happens to that material when it is obtained? If it is no longer needed for operational purposes, is it destroyed? Can we get clarification on that.

Ms Smith—Certainly. Derivative use of intercepted product is not really allowed. There is no provision in that legislation that allows law enforcement to collect TI product for general intelligence purposes. Therefore, TI product, unlike many other types of information that is collected by law enforcement, is not put in any centralised database. There are provisions within the act that make it an offence to disclose the existence of a warrant or to disclose the intercepted product, except for the permitted purpose for which it was obtained. For example, if information is obtained in relation to a particular drug investigation and there is another investigation happening within the organisation or within another organisation of which they have TI product, they may pass that information on.

I can give you an example. If, for example, the Australian Federal Police are investigating a drugs matter and they, as part of an intercept, receive information that is relevant to a murder that might be happening in the New South Wales jurisdiction, they may pass that information on for that purpose and for that purpose only. That is under section 68 of the act. If they receive information that is totally irrelevant to the offence which they are investigating or information that is not relevant—like another serious offence—that information must be destroyed. The act is quite clear on its destruction provisions. That has always been in there, basically. It is not any more relevant to device based warrants than it is to any other warrant.

There has been a lot of evidence given this morning about innocent parties and the intercept of their possible product. I point out that in relation to a device based warrant it says that once the purpose for that warrant is no longer in existence the warrant has to be revoked. So, if we think about that example that someone mentioned in their evidence this morning—that it might be a public computer, for example—the purpose of them intercepting that device is that they have had other surveillance that determines that they have seen a particular person sitting at a particular terminal who they believe is undertaking a particular crime, but they will

not have, say, the email address of that person. So that warrant will only be in existence until they find out that actual service. Once they have that email address, they can clearly go and obtain a warrant to intercept that service and revoke the warrant to intercept the computer that was in that public place—those sorts of concerns.

There is no derivative use of TI product except for those very limited grounds which are in the act, and that is for the permitted purpose of the original investigation or to pass it over for a relevant offence, which has to be punishable by at least three years imprisonment. So it is very, very tightly guarded. Certainly the AFP can talk more about their destruction provisions, but each intercepting agency has very strong accountability regimes inside such that they do have to destroy, and it is part of the role of those oversight bodies like the Ombudsman that they review and make sure that that has actually been undertaken. And, if not, then reports are made to ministers that they have breached their obligations to destroy particular information.

ACTING CHAIR—Mr Whowell, did you want to respond, or are you happy with that response?

Mr Whowell—I have nothing to add to what Catherine said.

Senator KIRK—Thank you for your submission. As you would have heard this morning, there is a great deal of concern amongst witnesses that under these provisions there is no additional scrutiny when there are additional devices added on to a warrant. I want to ask—and this is probably to the AFP—whether or not there are any operational limitations or any concerns along those lines that might prevent scrutiny by either a judge or an AAT member in circumstances where an additional device is to be added to a warrant. Perhaps you could outline for the committee those concerns.

Mr Whowell—I just need to be careful about how I answer that, so as not to reveal operational methodology. Ian will give me a heads-up if I start to stray. Our major concern is that during the course of an investigation and during the course of a warrant, as Catherine has indicated, during those 90 days, for example, we may become aware that somebody who is being intercepted under a named person device warrant has purchased additional devices and they are using those to evade our interception. Given the amount of checks and the processes involved in checking that they are using those devices and that they are legitimate devices—the actual tests that any internal certifying officer would have to be satisfied that adding to that warrant was within the scope of that warrant—that is a long enough process for us to get the window into the product that we might be missing out on while the person is taking that countersurveillance process. So that would be our concern: how much product we would use and how that might undermine our capability.

Senator KIRK—It is a matter really of the time involved. Is that your concern?

Mr Whowell—That is my understanding, yes.

Senator KIRK—But, the way you have just described it, there is no independent assessment or scrutiny by anyone other than that officer who makes the determination that it is necessary to add that device.

Mr Whowell—The AFP has very strict internal procedures in place generally to deal with TI. Those processes are set at a standard so that when we make an application with the DPP

before an issuing authority we have a high chance of success because we have met the tests in the legislation. So we have those processes in place and we have a separation between the person who is running the investigation in those processes and the person who is authorised to allow them to apply for the warrant in the first instance, and then that person who would then make an independent decision as to whether the investigator has met those grounds for a device to be added. So it is an internal authorisation process. We see that as the way forward because of those time constraints and the sorts of operational contexts that we would be looking at this for. That would then, I guess, be scrutinised at later stages of that downstream process through the role of the Ombudsman.

Ms Smith—I might just add there that the decision to add another device will be made by a senior officer within the agency, which does sit separately from any of the actual investigation itself, so the objectivity does come in there. I should also say that they will not be able to add a device that is inconsistent with the purposes of the warrant in the first instance. There has to be not only the likelihood that the person is using it but the likelihood that the use of it is in relation to the offence for which the warrant was issued. Also, the AAT themselves can actually place conditions, and this is regularly done. There has been a lot of comment on our reporting. You will see in the report that it is not unusual for conditions to be placed on warrants. The AAT use that conditional situation quite regularly in the named person warrant in the service context to remind law enforcement of the particular purpose and that no additional service, in the case of service warrants, can be added outside the parameters of their decision. So the AAT do have that level of accountability in the document that they issue that the law enforcement agency is subject to.

I should also say that, as a matter of best practice, the Attorney-General's Department must receive copies of all warrants. That was in amendments in 2006. It was taken away from the Australian Federal Police and put with the Attorney-General's Department. We have also required as a matter of best practice that in future, if any devices are to be added, we must be notified of that as well so that we keep watch from a legislative and policy perspective on additions. If we have any concerns we will of course go straight back to the agency, as we do with warrants currently.

Senator KIRK—You talk about conditions being put on the issue of warrants by, say, an AAT member, and you also talked about the fact that it needs to be consistent with the purpose of the original warrant, but, again, where is the check? Where is the independent check in relation to that? I understand what you are saying, that Attorney-General's are provided with a copy of it, but, from an independent point of view, where is the external scrutiny?

Ms Smith—There is not the external scrutiny. There is a scrutiny within the organisation. That is done because, on balance, it is considered that in the particular case being investigated there has been the satisfaction of an AAT member or a judge that the crime is serious enough to warrant the issue of a warrant and that, in this case, the activities of the persons are such—and they will satisfy the AAT member when they seek a device warrant that the activities of the person are such—that they have proven that they are the kind of person who is using multiple devices. So they have to satisfy that sort of information in the original affidavit. I do understand what you are saying, but I suppose I am saying that the integrity of the law

enforcement agencies is such that they do have accountability within their own agencies, and it is from a senior officer level that these are added.

Senator KIRK—Does the process you have just outlined apply to state agencies as well?

Ms Smith—Indeed, yes.

ACTING CHAIR—Is it consistent?

Ms Smith—Yes, it is. Because it is Commonwealth legislation, all 15 intercepting agencies—no, sorry, ASIO have different provisions, so it is all 14 law enforcement integrity agencies—are subject to the exact same provisions. All provide copies of warrants to Attorney-General's. All are subject to approaching the AAT or Federal Court judges, so it is the exact same system, and the guidance is centralised through the Attorney-General's Department on best practice. We regularly do reviews of best practice and review the systems that are in place. The last time that was done was in July last year, where a senior officer from my department went around and actually visited every single agency to check out their mechanisms for applying for warrants and also protections and those sorts of things, and he was satisfied on that.

Senator BARTLETT—I first want to go to comments you have made about what was always intended in the act and that these are just clarifying amendments. I appreciate that the department or even the government of the day may have had a particular intention, but I get puzzled, being a member of parliament, being told what the parliament's intention was a few years ago given what seems to me quite clear wording in the amendments that were made in 2006—which quite clearly state that 'telecommunications devices must be identified in the warrant'. How can you now say that it was the intention of the parliament to have at that time allowed interception of devices that were not identified in the warrant?

Ms Kelly—I was not actually around when these amendments were put in, but it is my understanding that the inconsistencies have arisen whereby the original warrant talks about a particular device; however, there are also provisions that allow for a device to be added after the fact. The main intention—

Senator BARTLETT—Sorry, I am not trying to be picky here, but I am trying to be precise. I accept that bits of the act specify that it can authorise interception of multiple telecommunications devices—that is there. But there is nothing that suggests that those multiple devices do not need to be specifically identified in the warrant, as far as I am aware. I was around in 2006 and, although I was not specifically responsible for this legislation, I kept half an eye on it. I do not think there was any specific comment made at the time by any minister that the intention was to allow further devices to be added that are not specified in the warrant. So I am just wanting some more solid basis of how you can ascribe intention to the parliament when it is not specifically there—and it was not specifically made clear in parliamentary hearings or anything else that I am aware of.

Ms Kelly—I can only comment on the intention of the department at that point in time. It was to introduce a service based named person warrant regime and a device based named person warrant regime—so basically separating out the existing named person warrant regime to allow for services and devices to be intercepted. We have gone through the reasons why we have separated that out, but they have also put in a higher threshold test for the device based

warrant regime. The intention at that time was that both regimes for named person warrants would be identical, that you would be able to identify multiple services on the face of the warrant and that you would be able to add services and devices to the warrant.

Senator BARTLETT—Can I suggest that there is a distinction between what the intention of the department may have been at the time and what the intention of the parliament may have been at the time. The parliament passes the law and we can only go on what is actually in the wording of the law.

Ms Kelly—Certainly, Senator. All of the documentation brought together and the explanatory memorandum are inconsistent. That is our view—that the intention at the time was to allow the multiple devices.

Senator BARTLETT—Could I at least suggest that it might not be accurate to say that it was the intention of the parliament.

Ms Smith—Yes.

Senator BARTLETT—Going to what is before us now, it might sound pedantic, but your asserting that these amendments are just making inconsistencies clear suggests that there is no big issue we have to deal with. From my point of view this bill does substantially change the situation—and you obviously would not be making the change if you did not want a substantial change. I do not want to tell you how to suck eggs, but I think it is problematic to suggest that these are just minor clarifications. Then when you discover they are not people naturally get a bit more suspicious that there is some other thing happening here. That is my piece of gratuitous advice for the day, for what it is worth.

On the broader issue there of whether the safeguards are sufficient, I appreciate that from a law enforcement point of view it is a lot easier to be able to just tack things on down the track without having to go back. On the initial accountability device, if you like, of the initial application for the warrant, I think you would have heard earlier today from the Law Council, which suggested that there should be four criteria: the person is a legitimate target of suspicion, the interception practice will be of some value, the device is likely to be used, and it is a uniquely identifiable device—and that is what currently has to be satisfied for the warrant issue. I do not think it is just a judge; it is the AAT or other people. Under this new regime, those last two criteria will not need to be satisfied. You will not need to satisfy the warrant-issuing officer that the device is likely to be used and that it is uniquely identifiable. What you are telling us, I think, is that you will satisfy yourself of that down the track, and you have got internal mechanisms to ensure that is done properly.

Mr Whowell—Yes, I guess that is half of what we are saying, in a sense. We believe that, for the addition of a device to an existing warrant, the internal accountability would be the way to go, and those additional oversight mechanisms would be through the reporting arrangements and the oversight of the Ombudsman and its scrutiny of our processes, which is fairly regular. It is annual and regular.

Senator BARTLETT—What seems to be the issue here, fairly clearly, is not so much that there may be multiple devices but that you do not need to get further authority to add multiple devices. I suppose I am a little bit wary even of just this incremental argument that is often used. You will tell us now, ‘Well, the intention is that we’ve just got to satisfy that the person

is worthy of surveillance and we don't need to satisfy the issuing officer that future devices are necessary.' I can see an argument being put in a couple of years time that, 'Oh, the intention was always that we didn't need to satisfy people that all the devices we were putting forward were necessary,' and that you would look at that yourself. I am just worried about another incremental shift in logic being retrospectively imposed upon us here. Why do you think then that it is necessary for the warrant-issuing person to be satisfied in the first instance that the devices you identify are necessary but that they do not need to be involved in being satisfied for future devices?

Mr Whowell—I guess the best way for me to answer that would be to say that, when you are seeking the grounds for the original warrant, you are at the earlier stage of the investigation. You do not have interception in place, so you are going through that accountability process. I do not think that anything we are saying or the department is saying is meant to undermine the importance of that up-front authorisation by an external body. What we are talking about is the fact that, in the overall architecture of the T(I) Act, a device based warrant is in the first place really the warrant of last resort. We have to be satisfied, and we need to be able to satisfy our internal processes and then the issuing authority, that a service based warrant or some other TI warrant is not a better way to get access to the information that we are after to assist with our investigation. As that investigation progresses and we are aware or become aware that that person suspects that they are under surveillance by the police, that the police are interested in them, and they start undertaking those countersurveillance type activities, we need to be able to try and counter that to maintain our capability. That is why we are suggesting that, when it comes to adding a device to an existing warrant where we were not aware of the existence of that device when we first sought the warrant, an internal authorisation approach, on balance with the other accountabilities that are available in the act, is the best way ahead from an operational perspective.

Ms Smith—It may be that at the time the application is put forward you are aware a particular person has, say, half a dozen devices but the details of the unique identifier are not known. That is why I was saying earlier that it is important we look at other forms of surveillance before we get to the point of applying for the warrant. There will be intelligence to say someone has walked into a particular shop and bought half a dozen phones plus 100 SIM cards, which is not an unusual scenario. The reality is that, until they use the phone, you cannot identify the unique identifier. It may be possible if it has been bought from a particular shop where they assist law enforcement, but in a lot of cases these are purchased from places that do not provide that sort of assistance. That sort of information must be in the head of the decision maker when they are making the decision. Law enforcement officers do have to convince others that this person has that behaviour. It is not enough to say, 'They have one device and we think they'll get some more later.' They would not succeed in getting a warrant. They would be turned away and told to get some other form of warrant. There has to be the behaviour to satisfy the original issuer that there is this type of use or access to these types of devices.

Senator BARTLETT—Under these changes, when you satisfy them that someone has a particular device and then you discover they have this other behaviour, you can add it all later. You do not need to satisfy the warrant issuer of the need to then add a whole swathe of

devices in the way you currently are. Going on your answer there, I assume that, under the current laws you are seeking to modify, when you go back to seek a further warrant for someone for whom you have already been successful in getting a warrant you would be required to seek to add further devices.

Ms Smith—We must apply for every warrant because the law as it currently stands—

Senator BARTLETT—Whether it is a new warrant or you are tacking new devices onto an old warrant, the effect is the same—you have to apply to get further permission and I presume they issue it. The point is really that justifying adding the device is not justifying the person because you have already made that case. You would be doing that already, I presume, sometimes.

Ms Smith—At the moment, each time a device is to be intercepted they have to go back with a completely separate application, completely from scratch. They may not get the same AAT member or the same Federal Court judge. They have to go back and apply for another one should there be a second device, which is why we are looking to clarify.

Senator BARTLETT—What sort of operational problem is that? I appreciate it is a bit of a drag. Even getting a different AAT member, a fresh pair of eyes looking at the case—is that necessarily a problem?

Mr Whowell—It is the overall time it takes to do it, not just one particular component. Getting a warrant approved is not a very quick process. There are checks that you need to go through. The carriers need to be able to put the intercept in place and all those sorts of things, which take time. We need to be satisfying the relevant legislative tests at the moment. If the people are engaging in behaviour to counter our surveillance of them, we are losing access and we may be losing critical information.

Senator BARTLETT—On the issue of uniquely identifying, you would have heard some of the evidence earlier today, particularly from Electronic Frontiers Australia, who basically said that it is less than precise. Could you indicate how you uniquely identify each device, any response you have to what they said and whether you have been involved in the development of a unique and indelible identifier for any sorts of communications.

Ms Smith—I am talking generally, not just about the AFP or intercepting agencies: before they can intercept communications they need to seek the assistance of the telecommunications provider to find out details of a particular service number—an IMEI in the case of a telephone or a MAC address in the case of computers. So they do these things called pre-warrant checks to seek subscriber information and that sort of thing to see if they can identify particular individuals—a unique identifier. If the carrier or provider who is providing this advice finds details—numerous of the same number, for example—then they will provide advice back to law enforcement suggesting that they obviously cannot uniquely identify that service and therefore they could not execute an interception warrant, should one be applied for.

In a policy sense, we are working with the industry, ACMA and the Department of BCDE to look at ways to deal with this problem. There are offences in the Criminal Code for altering IMEIs and IMSIs—being the service number or the actual phone handset number—and the AFP enforces those particular laws in relation to changing IMEIs and IMSIs. But, of course, technology is very fast moving and people will always find ways to change numbers. For

example, if a mobile phone is lost or stolen, the first thing the owner will do is get their IMEI blocked so that the phone will be of no use to the person who found it. Therefore, if someone happens to want to use the phone, they are going to seek out someone who can change that IMEI so it can become unblocked.

So there is work on foot to try and deal with the issue, and certainly there are lots of organisations that we work with trying to deal with the issue, but it is a very difficult one. In relation to the integrity of law enforcement, they are required to do pre-warrant checks before they even apply for a warrant, to satisfy themselves of the uniqueness of the particular number.

Mr Wilson—I will add to that without getting into too much detail which will give away our operational techniques. If, for example, there were a phone with a cloned IMEI or equipment identifier, one way of identifying it would be to take other information into account—maybe surveillance, which gives the location. If there is a clone of a person's phone then you have two bits of information, which is making it unique in that it is separating the phone in this location and maybe the real subscriber's phone in another location. So there are other things we can do to get a unique identifier in those cases where there is a cloned IMEI—equipment identifier.

Senator BARTLETT—What about MAC addresses? It seems to be somewhat easier, as I understand, without giving away tips.

Ms Smith—Actually, I have heard that MAC addresses were not easier to modify, so I cannot comment on that. I had heard it was the other way.

Senator HOGG—Could I just follow up there. If this goes to operational matters, I will understand that you will not be able to answer, but are you able to give me the number of surveillances that are jeopardised by you not having the facility? I do not want to know if it is five or six, but are you able to give an order of number? And what about the frequency? In other words, is it daily, weekly or monthly? I would like to get some sort of sense.

Mr Wilson—I guess the other thing is the importance of the operations—do these tend to be things that involve people with a high level of technique or a high level of understanding of technology who are probably committing more serious crimes? I could provide that information later on in confidence, but I do not have it at the moment.

Senator HOGG—So you will address those issues. If that is confidential, you can mark it confidential, but I think it would help the committee to get some idea of the frequency, the nature and the quantum of surveillances that are jeopardised by not having the facility that is being sought under this legislation.

Mr Wilson—If we could have a couple of weeks to do that, that would be helpful.

ACTING CHAIR—You can take that question on notice.

Ms Smith—We will seek that information as quickly as we can, and we may ask a couple of other agencies to assist as well.

ACTING CHAIR—I just note that our reporting date is 30 April.

Ms Smith—Yes, I am well aware of that, so we will get that back to you as quickly as we can.

ACTING CHAIR—Thank you.

Senator BARTLETT—I will try and be brief. I have a question on one other matter: the issue of the sunset clause and intercepting and the like. I think you have had some questions on that already. Firstly, the exemption applies to law enforcement agencies. Is there a concern that other agencies or indeed private enterprise might be technically in breach of the act in things like virus scanning and email quarantine systems?

Ms Smith—The nature of computer networks is so different and complex that I could not comment on whether particular areas of industry or banking or whatever would be in technical breach of the act. What I can say is that when it is appropriate we constantly provide guidance to organisations when they ring up and talk about their filtering systems. You will find that a lot of organisations actually straightaway block emails of a particular attachment type because they know that they are likely to have problems embedded, even though they might be quite innocent. They also run electronic scanning, which is not in breach of the legislation. But we have identified that this is an area that is grey and that needs to be dealt with as quickly as we can. Certainly I am not aware of any organisation that is in technical breach of the legislation. As I have said, we welcome people to approach the department and seek guidance on how they can actually act and not be in breach of the legislation and still protect their networks.

Senator BARTLETT—Can I just go to the issue of some of the media commentary in the last couple of days. It is not in the bill before us, so I do not want to spend too long on it, but you did bring it up yourself. Again, I am a bit wary about motive being retrospectively prescribed to parliament on the basis of passing comment, so I will clarify the general intent. I note comments, for example, from the then Acting Prime Minister, Ms Gillard, that these measures are about looking at critical infrastructure and making sure that our banking system is safe from terrorist attack and these sorts of things. How does that match what you said earlier in your introductory remarks about what is being planned here?

Ms Smith—I think it is consistent. We are certainly looking at it from a very broad perspective. That is why we are working with our critical infrastructure protection area, which has a very good understanding of the banking sector and all the emergency services as well as electrical grids and that sort of thing. What we are doing is, I suppose, future-proofing the legislation. Perhaps one of the reasons you see us back quite regularly is that the technology is moving very fast. What we are seeking to do is ensure that, as technology changes in relation to network protection, there will not be these potential technical breaches in the future if they do exist, so we are looking at it very broadly. The provisions as they stand at the moment also deal with professional integrity within the particular agencies, of which the AFP is one, and that certainly will continue in the current state, but we are not looking at that being broader than those agencies that it currently applies to in relation to the professional standards issue. What we are looking at is network protection for the whole Australian computer network, in effect.

Senator BARTLETT—So when you are talking about private sector network protecting you are basically talking about electronic attacks against the integrity of a network. You are not talking about—in very crude terms—monitoring the content of emails to see whether there is a terrorist talking about bombing the Sydney Harbour Bridge?

Ms Smith—No. That would have to be subject to interception warrant.

Senator BARTLETT—That is basically what is already there.

Ms Smith—That is correct. This is about network protection.

Senator BARTLETT—So when you use terms like infrastructure you are actually talking about the infrastructure of the network.

Ms Smith—Yes, that is right. I think of the physical infrastructure of computer networks that have bits and bytes flying past. We are hoping to ensure that there will not be nasty little things embedded in those bits and bytes that can bring down a whole electrical grid or our banking systems, all the things that we treasure quite deeply now online.

Senator BOB BROWN—Do you really think there is a long-term solution for network protection or do you think that is going to have to keep moving too?

Ms Smith—I hope we can come up with a solution that is technologically neutral and will apply as networks evolve so we do not get caught in this position of having to come back and make some changes. The reality is that the types of attacks on networks are changing all the time. That is why there are attacks, I suppose, because as soon as there is a solution established all you need to do is put in a firewall or something to bounce that particular problem that comes forward. A solution will allow the people who need to stop those malicious attacks coming through to be able to do their job without being in breach of the legislation. As far as my area in the department is concerned, because we administer the TIA Act, we are ensuring that whatever is done in the future by network people to protect their infrastructure and the Australian public—and they need to be protected when using things online—is not going to be in breach of the act. I would hope that any solution we work on will actually achieve that.

Senator BOB BROWN—Do you really think that is possible within 18 months from go to enactment?

Ms Smith—Should I say that I am optimistic?

Senator BOB BROWN—I might like optimists, but—

Ms Smith—I believe that we are getting to a good state at the moment with developing a position that we think is a good start for consultation. Once we start consulting, I think it is only then that we will really establish what the interested stakeholders see as the true problem. It is being given a very high priority by the department to move it forward. Again, of course, we are subject to parliamentary programs, so if there is an agreed solution it will depend on our ability to get it before parliament and get government agreement to take it forward in the first instance. We are optimistic that 18 months is the correct amount of time. It also gives us the pressure we need to push the matter forward as quickly as we can.

Senator BOB BROWN—Otherwise we will be here again in 18 months.

Ms Smith—We might be. I hope not.

Senator BOB BROWN—Just finally, the other section that has been under scrutiny here has been the business of not having to go back to get a new warrant to cover a new device. Does that also apply to devices that are not bought by the target of surveillance but maybe by their friends, relatives or acquaintances or that may indeed be public devices?

Ms Smith—That is correct, yes. But, still, if we are talking about the addition of it, the decision maker will have to be satisfied not only that the person is using or is likely to use that service but that it is likely to be connected with the commission of the offence. It is not enough to say that the person is just likely to use it; it has to actually be used in the commission of the offence. There is that sort of double-barrelled thing. That is quite correct. A regular way to avoid detection is to pass phones or services around.

Senator BOB BROWN—But you do not have any worry with the balance of probabilities test?

Ms Smith—I am satisfied that the tests within the legislation are enough to protect the privacy of individuals using the telecommunications network.

Senator BOB BROWN—Would you be prepared to look at the balance of probabilities test?

Ms Smith—As being the test rather than the likely—

Senator BOB BROWN—Yes. I know that needs some thinking and perhaps you could come back to the committee with comments on that proposition.

Ms Smith—I am certainly prepared to take that on notice for you.

Senator BOB BROWN—Thank you.

ACTING CHAIR—I would just like to finish off with a couple of questions. In terms of the consultation process for this bill, have you consulted with the relevant law enforcement agencies? I am thinking in particular of the state agencies.

Ms Smith—Most certainly. We have consulted with all of the interception agencies, yes.

ACTING CHAIR—Do overseas examples—and I am thinking of the UK in particular—have similar legislation? What is their model and can you describe it?

Ms Smith—It is called RIPA, the Regulation of Investigatory Powers Act 2000. It has provisions for the interception of services as well as persons and devices. They pretty much cover the whole ambit of what we do. The very major difference with the UK is that they are non-evidentiary based, so they have very different provisions when it comes to retention of the interception product. They do not actually put the information into evidence, so they have very different approaches as to how they collect the information, how it is passed on and how it is used. I have to say that, as far as all international jurisdictions go, Australia has the most accountability within it. We are one of the few jurisdictions that have a full annual report. Most other jurisdictions do not.

ACTING CHAIR—Which annual report are you talking about?

Ms Smith—Our interception act annual report. Most other jurisdictions do not provide statistical analysis, and those that do provide statistical analysis do not provide it for every warrant issued, like we do. I have not given you a rundown on exactly what RIPA does, but certainly most European jurisdictions can intercept on devices. But, again, it is a bit like comparing apples and oranges, because they have different approaches. We also have a higher threshold for our offences. We have a minimum of seven years except in cases of particular child pornography offences and some other computer type offences—money laundering maybe. Most other jurisdictions have a much lower threshold than ours. I think most have about a three-year threshold. If you want me to take on notice any specific questions, I will. It is a very large piece of legislation.

ACTING CHAIR—Indeed. Obviously we do compare with the UK. If you had a view of the UK in terms of how they handle the addition of devices, the committee would welcome advice in that regard. Can you take that on notice?

Ms Smith—Yes. I will take that on notice, most definitely.

ACTING CHAIR—On page 4 of your submission, in the second paragraph—this was raised by the Castan centre this morning—you refer to this delegated officer who is entitled to approve or not approve the additional device. How does it apply in different law enforcement agencies? Is there a consistent approach across all law enforcement agencies?

Ms Smith—It very much depends on the size of the law enforcement agency. You will appreciate that in New South Wales alone there are four intercepting agencies. When it is a small agency, it is more likely that it is the chief officer who will actually sign off things. In the New South Wales police, because of the size of the organisation, it is delegated a little further down. But, as I mentioned earlier, we have gone around to each of these agencies and satisfied ourselves that they are beyond reproach and that the integrity of their systems is good.

ACTING CHAIR—But, with respect, you are asking us as parliamentarians to sign off legislation where we do not actually know the identity of the authorising agent in each enforcement agency.

Ms Smith—Yes.

ACTING CHAIR—What do you say to that concern?

Ms Kelly—It is always the head of the agency or the deputy head of the agency, and then it can be an SES equivalent who is authorised in writing by the head of that agency. So, depending on the size of that agency, there may be four officers authorised in writing in a medium sized agency. There may be 10 in a larger agency. It does come down to operational efficiencies, but that accountability is held at the SES equivalent level or higher.

Ms Smith—We should also say that it is centralised.

ACTING CHAIR—Are they identified? Are they known?

Ms Smith—Yes.

Ms Kelly—Yes, they are.

ACTING CHAIR—To who?

Ms Kelly—Within the organisation, it is an officer authorised in writing. There must be a document.

Ms Smith—But it is not a public document as to who is actually authorised. The information is held within the agency. I should also say that it is centralised to a particular point within an agency as well. In the bigger organisations, they actually have specific interception divisions. It will only be senior officers within that area that have this responsibility. In a smaller agency, there will only be two people in that interception division and it will be their commissioner who actually signs off on it.

ACTING CHAIR—Mr Whowell, did you want to respond?

Mr Whowell—I would just add to what Catherine and Wendy have been saying. It is not just the size of agency but also the geographic spread. In terms of the certifying or authorised officers in the AFP, that is what we need to take into account. Those people are authorised in writing and are SES equivalent or above.

ACTING CHAIR—Thank you very much. I have a final question. It may be a very simple one. In terms of this legislation, we obviously do not need any complementary state or territory legislation, do we?

Ms Smith—No, except in relation to the ministers. If they choose to opt in and receive a copy of a warrant, they will have to amend their own legislation to allow for that.

ACTING CHAIR—I think that is a very relevant point. They will need to pass their own legislation to opt in; is that correct?

Ms Smith—That is correct.

Senator HOGG—The question is: by when? Given that the sunset clause on this is 30 June, as I understand it, would they need to have complementary legislation operating prior to 30 June?

Ms Smith—No, they will not. Because it is an opt-in situation, it will be up to each state jurisdiction to decide whether they want to take forward their legislation, and they will do it under their own legislative program. We have been consulting with the states and the offices of the state ministers on this issue.

Ms Kelly—The amendments actually allow for information to continue to be provided to the state ministers until such time as, and then after, they get their own state legislation in place.

ACTING CHAIR—Are there any concluding comments?

Ms Smith—No.

ACTING CHAIR—Thank you very much for appearing before us today. It is very much appreciated. In closing, I would like to thank all the witnesses who have given evidence to the committee today.

Committee adjourned at 12.41 pm