COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL AFFAIRS LEGISLATION COMMITTEE

Reference: Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010

THURSDAY, 11 NOVEMBER 2010

CANBERRA

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://parlinfo.aph.gov.au

SENATE LEGAL AND CONSTITUTIONAL AFFAIRS

LEGISLATION COMMITTEE

Thursday, 11 November 2010

Members: Senator Crossin (Chair), Senator Barnett (Deputy Chair) and Senators Furner, Ludlam, Parry and Pratt

Participating members: Senators Abetz, Adams, Back, Bernardi, Bilyk, Birmingham, Bishop, Boswell, Boyce, Brandis, Bob Brown, Carol Brown, Bushby, Cameron, Cash, Colbeck, Coonan, Cormann, Eggleston, Faulkner, Ferguson, Fierravanti-Wells, Fielding, Fifield, Fisher, Forshaw, Hanson-Young, Heffernan, Humphries, Hurley, Hutchins, Johnston, Joyce, Kroger, Ludlam, Macdonald, McEwen, McGauran, Marshall, Mason, Milne, Minchin, Moore, Nash, O'Brien, Payne, Polley, Ronaldson, Ryan, Scullion, Siewert, Stephens, Sterle, Troeth, Trood, Williams, Wortley and Xenophon

Senators in attendance: Senators Barnett and Crossin

Terms of reference for the inquiry:

To inquire into and report on: Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010

WITNESSES

Committee met at 1.34 pm

CHAIR (Senator Crossin)—I declare open this public hearing for the Standing Senate Legal and Constitutional Affairs Legislation Committee and our inquiry into the provisions of the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010. This bill was originally introduced by the Attorney-General in the House of Representatives on 24 June 2010 and referred to the committee, but of course the bill lapsed when the 42nd Parliament was prorogued. The bill was reintroduced by the Attorney-General in the House of Representatives on 30 September. On that day the Senate referred the provisions of the bill to this legal and constitutional affairs committee for inquiry and report by 24 November.

I want to 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 the 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 the committee. We do prefer all evidence to be given in public, but there is provision for witnesses to actually be heard in private sessions. If you want to do that you will just need to approach us and we will arrange that. If you as a witness object to answering a question then you should state the grounds upon which the objection is taken and the committee will determine if it will insist on an answer, having regard to the grounds which are claimed. If the committee determines to insist on an answer then the witness may request that the answer be given in camera. I welcome our first witnesses for this inquiry.

[1.40 pm]

ALTHAUS, Mr Chris, Chief Executive Officer, Australian Mobile Telecommunications Association

ELSEGOOD, Mr Michael John, Manager, Regulatory Compliance and Safeguards, Optus

RYAN, Mr Michael, Manager, Future Networks and Services, Telstra and appearing as Member, Communications Alliance/Australian Mobile Telecommunications Association and Internet Industry Association

WILSON, Ms Peppi, Manager, Policy, Australian Mobile Telecommunications Association

Evidence from Mr Elsegood and Mr Ryan was taken via teleconference—

CHAIR—Welcome. The Communications Alliance, Australian Mobile Telecommunications Association and Internet Industry Association have lodged a submission with us, which is No.2 for our purposes. Are there any amendments or alterations that need to be made to that?

Mr Althaus—No, Chair.

CHAIR—I invite you to make a short opening statement, then we will go to questions. I am not sure if all of you have something to say or someone is going to say it on behalf of all of you, but we only have about 20 to 25 minutes so I would ask you to make it brief.

Mr Althaus—Thank you, Chair, and thank you for the opportunity on behalf of the three organisations. We are here to speak to the submission and answer questions from the committee. To keep it brief, the industries or the sectors of the overall communications industry which we represent regard very highly and take very seriously the roles that we are able to play in working with Australia's law enforcement agencies and related government departments. We are actively involved and have a very strong and close relationship stretching back many years. In fact, we are in one of the most dynamic and a rapidly changing sectors in the economy and this presents a range of challenges to all involved, including industry and law enforcement agencies, when it comes to issues related to interception.

I should say at the outset that industry was not consulted on this bill during its genesis. When we were able to look at the content, fundamentally the industry had no particular comment on schedules 1, 3, 4, 5, 6 and 7. Our particular concerns relate to schedule 2. In that schedule the communications access coordinator is able to prevail upon the industry or proposed to prevail upon the industry to notify of new procedures. It is the concept of this schedule and its implications that are of greatest concern to the industry. Given that this schedule requires us to provide advance notice, one of the issues that has come clearly to our mind is that industry already does this in great measure. In fact, in this place as recently as 29 October, in a Senate Environment and Communications References Committee hearing, a senior Attorney-General's Department official stated:

> Industry are very good in coming to us and giving forewarning on when technology is going to change that may have an effect on law enforcement's views. They are always wanting to make sure that we can keep pace with technology; they are very helpful in that respect. Given that they service a lot of requests from these particular databases—

et cetera. This is a reflection of the close relationship that exists and has done over time.

Moving to the nature of the environment in which this is taking place, I inform the committee of very, very significant growth and dynamic shifts within the industry, and it is the online environment that we are referring to. Figures out today by the Australian Communications and Media Authority suggest that over 50 per cent of the population are now regarded as heavy to medium users of online services, spending a minimum of seven hours a week online. Of course, the access and availability of information in cyberspace is one of the greatest challenges for law enforcement and it is one of the more difficult aspects for local industry in terms of meeting interception requirements put into existing legislation.

Schedule 2 in this bill should not proceed, we suggest. It is a schedule that will impose what we regard as onerous requirements on industry and has the potential to limit partnerships and outsourcing by Australian companies. It creates a non-technology neutral situation with uneven requirements in Australia versus other places in the world. It will certainly create uncertainty and high levels of risk; it certainly will delay and potentially limit the roll out of innovative products and constrain the ability of our members and the industry to assemble competitive packages. Why is that the case? It is simply because the vast majority of online material can be accessed by people outside this country.

I will give you an example in the mobile telephone space. There are now some 500,000 mobile applications available on the market, the vast majority hosted outside this country. Globally, 28 million to 30 million downloads take place every day of those applications. With such a rapidly changing environment it would be very difficult, given the constraints in schedule 2, for the industry to be free to respond to the dynamics in terms of product release et cetera in the market.

I underscore that with those comments we do not resile one bit from our responsibilities to be of assistance to law enforcement agencies. We understand the value of their input. We are committed to retaining that. Australia is a standards taker in this global marketplace. It is highly competitive. We are concerned about the impact of schedule 2 in this bill on competitive capacity, on risk and on the timely ability to deliver products that are increasingly a fundamental part of the lives and lifestyles of Australians—as they are all around the world.

In addition, there are existing mechanisms within existing legislation that we believe could be amended so as to have as good an effect, if not a better one, than the changes proposed in schedule 2. We particularly identify the use of an interception capability plan, which is already required. Amendments to the ICP arrangements would be, in our view, a simpler way to achieve the kind of outcomes that schedule 2 attempts to achieve.

Schedule 2 gives the communications access coordinator essentially a power of veto. We could see a situation in which changes are delayed in the first instance by 30 days and possibly by another 30 if there are questions to be asked. These sorts of delays in the dynamic and very rapidly moving industry environment that we are talking about would be a significant impediment for Australian industry. Bear in mind that consumers need not pay attention to Australian industry; they can simply source this material from other places in the world over the World Wide Web.

I am going to pause and ask Mr Ryan to perhaps give examples and talk a little further about the way we currently cooperate with agencies and how schedule 2 is going to be a very challenging part of this bill should it proceed.

Mr Ryan—Presently, the larger providers in the telecommunications industry have a very good and cooperative approach, regularly meeting with and talking to the agencies to brief them on new technologies and advances in telecommunications services and applications. This is in addition to—particularly with my organisation—our weekly meetings with the agencies to talk to their technical staff on operational and engineering issues that may impact on our capability to respond to agency requests. We also update, on a regular basis, the agencies, particularly at the Communications Security and Enforcement Roundtable, which is run by the ACMA, and also the expert group, which a lot of our senior managers attend on a regular basis.

I will refer to the interception capability plan. The interception capability plan is an obligation on all carriage service providers to provide a report to the Attorney-General's Department or the communications access coordinator every 12 months. In that interception capability plan we are required, particularly under section 195 of the Telecommunications (Inception and Access) Act, to provide a statement on any relevant development in the business of the service provider within a five-year period that may be implemented by carriers and likely have an effect on our interception capabilities.

My particular organisation, in our 2010 interception capability plan, identified 104 new products and services which we would be launching from the 2009-10 financial year. Of those, we identified 17 which were brand new and which may have an impact on our interception capability plan. Of the other 87 products and services, we determined that there would be no impact or our existing capabilities would take care of that interception obligation. We believe that schedule 2 is going beyond that and placing a further large reporting burden on industry when in fact the interception capability plan appears to be working quite well at the present time.

Mr Althaus—Chair, could I add to those comments. One of the emerging areas in the industry and more broadly is cloud computing. In this example, cloud computing could trigger the need to notify locally. But of course cloud computing, by its very nature, does not adhere to geographic boundaries. I know Mr Elsegood is emersed in this. Perhaps, Mike, you would like to take that example forward.

Senator BARNETT—Perhaps you could explain what cloud computing is.

Mr Elsegood—There are a number of providers, who are largely located outside of Australia, who have cloud computing applications.

Mr Althaus—Mike, could you just explain what cloud computing is, please.

Mr Elsegood—Sure. Cloud computing ranges from the simplest task of storing people's information online, such as photographs and documents, through to hosting applications like word processing and spreadsheet functionality on the internet instead of having to buy specific programs to do that on your computer. Quite sophisticated programs can be hosted on the internet or on a computer connected to the internet instead of having to buy the application yourself. You almost use them on a pay by the minute approach, instead of having to pay a licence fee for software. As I said, there is a whole range of complexity through the cloud computing marketplace.

Providers in Australia can be telecommunications related companies or independent software related companies. So we end up with some real discrepancies with what is proposed in schedule 2 in that if a telecommunications company wants to package up some cloud computing with some of the telecommunications services that it is providing it appears to get caught up in schedule 2 but a purely software house doing the same sort of thing apparently does not. Likewise, these services can be supplied directly from overseas. But if we want to become involved and make it easier for our customers to put together a total package of services we seem to get caught up with the additional notification required through this process. I might leave it there.

Mr Althaus—Chair, with time in mind, we will draw our comments to a close by simply saying that we were disappointed not to be consulted on this new bill, particularly in relation to schedule 2 as it has significant potential to impact upon the industry. We are already acting, in a way, under the ICP plan which mirrors, in many respects, what is required, and the relationships between industry and the agencies concerned are seen to be effective in this regard. I point out to the committee that the use of the determination in the existing legislation has been very, very sparse. In fact, it has rarely been used in recent times, so we question the need for a wholesale change introduction to the very new regime, as proposed in schedule 2.

CHAIR—I might start by asking you to clarify something for me. In your submission you say that schedule 2 now establishes new procedures which must comply whereby the carriers must notify the Communications Access Coordinator of network and system changes that impact on interception capability. Can you give me an example of what a network or system change would be.

Mr Althaus—I certainly could but I will ask the technical gurus.

Mr Elsegood—Under the very expansive definitions of what constitutes a telecommunications service and a telecommunications system under the TIA Act, a system change could be something as simple as a particular cloud computing application which has been packaged together for targeting to smaller and medium business customers, or it could be something as extensive as a wholesale change to shift to, say, a major in-house computing application from being hosted on a computer in Australia to being hosted onto a computer somewhere overseas.

CHAIR—Can you give me an idea of how many of these network or system changes occur either, say, weekly or monthly.

Mr Elsegood—We are doing changes all the time in our organisation. We are looking at adjustments to products. We are looking at new services and applications all the time. We do not know the extent of just how much reporting we would have to do under this proposed schedule. Part of our concern is that we would have to go back into our organisation and do a complete audit of the things that we do in order to make sure that we comply.

CHAIR—When you say you look at network or system changes, as opposed to them actually happening, I am trying to get a handle on how many there are. Are we talking about 10 a week or 10,000 a week? How does that differ from what you are now asked to do when you notify the Communications Access Coordinator?

Mr Elsegood—Perhaps we could take on notice the quantification of the number of changes, if possible.

CHAIR—You can see where I am coming from. I am trying to get a handle on how onerous or otherwise it is going to be. You allege that this will increase the regulatory and economic burdens on carriers, but I am just trying to get a handle on how significant that is going to be.

Mr Althaus—A good way of looking at this is that, at present, industry examines its business and provides, as we have said in the earlier statements, advice to agencies about changes that they might like to consider. What we have now is a proposed situation that is not clearly defined in the legislation, I would have to say. Let us say that it is down to industry to make an objective judgment on what might be worthy of raising with the access coordinator. We will do that under this arrangement, and then we have to wait for 30 days. If we do not hear anything after 30 days then we can proceed. So we have moved from an environment where we are

looking to keep agencies informed to a much earlier intervention. One of the fundamental problems we have is that, as such an early intervention takes place, you could well find that the market opportunity, the supply of the particular service et cetera passes by while we wait for an okay, if you like, to proceed. So there is a very strong sense that we are already doing this, in a sense, via the interception plan, but it is seen to not be impeding business processes too much. Moving back down the chain one or possibly two months is seen as being far more onerous and problematic in a business supply sense.

Ms Wilson—It is making more formal what is already going on with the meetings that the industry is having. The meetings are informal; this is putting a reporting formality on it. That is an extra impost.

CHAIR—So you are not suggesting that schedule 2 be deleted; you are just suggesting that it should be deferred till there is further discussion.

Mr Althaus—I think there is a very important point here: that this has significant operational challenges to it. So yes: we would want much more detailed discussions with government about how this might look or even how you might amend existing parameters rather than bringing a whole new schedule into place. Bear in mind that this goes to the level of the ability to compete within Australia, because, as I say again, a very significant volume of the applications and services that are accessed over the net would not be captured by this legislation in the sense that they are offshore and can be accessed by citizens over the web.

Senator BARNETT—Thank you very much, Mr Althaus and colleagues. You have a very thoughtful, comprehensive submission and some very valid points. We are just trying to get our heads around how onerous and cumbersome this would be and what level of impediment it would be to the commercial operations of your business. My understanding of what you are saying is that you now have to act in advance. You have these 30-day periods that are floating, where things can happen and change and you are left in limbo in a way. In the fast-moving industry which you are in, commercial opportunities can pass you by, and therefore competitors elsewhere can jump the gun on you. Is that right? What is the level of concern here? It sounds like a high level of concern you have.

Mr Althaus—It is indeed a high level of concern, particularly because it is a global marketplace and we are, although vibrant, a very small market in the overall global scene. The ability to compete and the enabling nature of the technology we are talking about could feasibly be quite a constraining element on the provision of service. It certainly has a cost risk and investment implications for industry, but that flows through to the availability of applications and services to the community and to consumers, be they individuals, businesses or even, dare I say, governments.

Senator BARNETT—So under the current arrangements you do advise the law enforcement agencies of your change of plan, but that is post facto.

Mr Althaus—It is, and we are saying simply that we should look again and would be interested in looking again at what we currently do and seeing how that might better be modified to meet agencies' needs, rather than throwing a blanket coverage over changes. I say too that there are some vagaries in here. We are not quite sure how the judgment is made. We are presuming that judgment on the need to inform is left with the carrier or the nominated carriage service provider.

Senator BARNETT—Would you like, either now or on notice, to put to the committee specific changes to the current arrangements or improvements you would prefer to the procedures set out in schedule 2?

Mr Althaus—The time spent with this bill has been limited. I think we are best simply making the offer, having not been consulted on this bill and particularly on this schedule, that industry stands ready to work through how we might achieve the outcomes government is seeking without necessarily going to what we regard as an onerous schedule in this proposed bill.

Senator BARNETT—With previous legislation, when bills have come forward, have you been consulted?

Mr Althaus—We have been putting ourselves forward as wanting to consult the whole way along, but the short answer would be no. In fact, the experts group that was referred to earlier was specifically put in place to try to up the level of consultation.

Senator BARNETT—Are you in that group?

Mr Althaus—I am, as are the other members of the delegation I am representing. So it is certainly an open offer from an industry perspective. We are very, very anxious that our responsibilities, our assistance and our ability to help are maintained and assisted.

Senator BARNETT—I will put it this way: would you be confident of getting to a mutually agreeable outcome with the department and the relevant authorities—if you had time to consult and work with them in a workshop style or whatever—if schedule 2 was either deferred or not proceeded with?

Mr Althaus—Confidence is relative, but we would certainly like the opportunity, and it is important that we be given the opportunity rather than having the schedule just proceed.

Ms Wilson—We have done it with other issues involving law enforcement agencies when a draft determination has been put out, and we have worked through unintended consequences of that draft determination to come up with an outcome that is much better for industry than the original proposal and that agencies and departments have been very happy with as well.

Mr Ryan—We had some very good outcomes, particularly in discussions of determinations that were issued by the Australian Communications and Media Authority and particularly around bomb disposal. We are currently in discussions with them and are very close to an agreement on the installation of jamming devices, particularly in the New South Wales prisons.

Mr Elsegood—I would like to refer back to one of the comments on the interception capability plan process. Where there is a substantive change to our networks which we are aware of, the interception capability plan process requires that we signal that forward. We also give a five-year estimate of what we see on the horizon, which we include in the interception capability plan each year.

Ms Wilson—Probably another point worth raising about that 30-day period is that even once you have gone past the 30 days and assume you have clearance, the CAC is able to come back at any point and say that they are not happy and that they require interception capability, even once the service or product has been launched. So it does not provide the business certainty that the media release, I think—or maybe the explanatory memorandum—mentioned in saying they can meet their obligations without the need for costly alterations. That certainty is not actually there when you read through schedule 2.

CHAIR—I do not have any other questions for the four of you. Thank you very much for your submission. Mr Elsegood and Mr Ryan, thank you taking the time to be on the end of the telephone for us.

[2.10 pm]

PILGRIM, Mr Timothy, Australian Privacy Commissioner, Office of the Australian Information Commissioner

CHAIR—Welcome. The Office of the Australian Information Commissioner has provided us with a submission which we have designated as No. 13. Do you need to make any additions or amendments to it?

Mr Pilgrim—No.

CHAIR—I invite you to make a short statement and then we will go to questions.

Mr Pilgrim—I welcome the opportunity to offer some opening comments to the committee on the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010. The Office of the Australian Information Commissioner understands the main purpose of this bill is to enable greater cooperation, assistance and information sharing within Australia's law enforcement and national security communities. It is intended that the bill will achieve this by amending the Telecommunications (Interception and Access) Act 1979, the Australia Security Intelligence Organisation Act 1979 and the Intelligence Services Act 2001.

The office recognises that the public interest in law enforcement and national security agencies sharing information to facilitate their legitimate activities needs to be balanced with the public interest in protecting the personal information of individuals. In achieving this balance, the office believes the proposed amendments contained in the bill should be limited to only those that are required to facilitate necessary information sharing and have adequate privacy protections in place. This approach will assist in building community trust and confidence in the bill.

At the outset, I would note that the application of the Privacy Act 1988 to those Australian intelligence agencies, Australian government law enforcement agencies and state law enforcement agencies covered by the proposals in the bill varies, thereby leading to some potential gaps in privacy protection. The office is interested in ensuring the consistent application of sound privacy principles in relation to these proposals, coupled with oversight by the appropriate regulator. To this end, we have made a number of recommendations in our submission to improve and enhance the privacy protections in the bill. I will briefly outline and highlight the main recommendations.

Firstly, the office recommends addressing potential gaps in privacy coverage which may occur in the handling of personal information obtained through an interception warrant. The office suggests developing guidelines on personal information practices for law enforcement agencies, which may assist in addressing these issues. Similarly, it may also be appropriate for the Attorney-General's Department to consider reviewing the guidelines issued under section 8A of the Australia Security Intelligence Organisation Act 1979.

Secondly, the office has made a range of suggestions to further enhance the privacy safeguards contained in schedule 3 of the bill relating to the disclosure of telecommunications data relating to missing persons. This reflects the office's view that sound privacy protection should apply when authorising the disclosure of telecommunications data for purposes other than investigating criminal activity. In particular, the office has suggested introducing a set of binding rules or regulations to apply to the handling of telecommunications data and developing detailed guidance on issues surrounding consent within the context of investigating missing persons.

Thirdly, the office recommends that, in relation to the proposed amendments contained in schedule 4 of the bill, regarding stored communication warrants, guidance be developed to assist law enforcement agencies to determine when a person is unable to consent or when it may be impracticable to gain consent. The office also suggests that the explanatory memorandum to the bill expressly canvass privacy issues that may arise within the context of these proposed amendments to assist the issuing authority when considering the factors set out in section 116(2) of the Telecommunications (Interception and Access) Act.

The office further recommends the establishment of a privacy framework to support the information sharing arrangements set out in schedule 6 of the bill to overcome any potential gaps in privacy protection. This framework could be established through the development of a memorandum of understanding between participating agencies and could include personal information handling guidelines covering the collection, use, disclosure, accuracy, storage, security, retention and destruction of personal information and complaint handling. Again, doing so could also assist to further enhance accountability measures and improve transparency and public confidence in information handling processes under the proposed reforms.

Finally, the office suggests that schedule 3, which deals with the disclosure of telecommunications data relating to missing persons and schedule 6, which deals with the sharing of information between intelligence and law enforcement agencies, contain a statutory review mechanism to ensure the operation of the personal information handling requirements under the proposed amendments in these schedules are reviewed and assessed after a period of time. Adopting such an approach would augment existing accountability mechanisms.

In these brief opening remarks, I have focused on aspects of the bill which the office believes are the most relevant to safeguarding the privacy of individuals while ensuring the facilitation of necessary information sharing between intelligence and law enforcement agencies undertaking their legitimate functions.

Senator BARNETT—In regard to schedule 3 and schedule 6 and the need to establish a sort of privacy framework around those, how extensive would that be, how necessary is it and how long would it take to draft, prepare and put in place that framework?

Mr Pilgrim—The questions of how long it would take, how necessary it is and how extensive it should be are quite broad. What we would like is to see the most consistent approach to the handling of personal information within government agencies of any type. The Privacy Act, as you are well aware, provides a framework for doing that and sets out principles in different parts of the act about how organisations can best collect and handle information and use it in certain circumstances. We think those principles would form a good basis for looking at any guidance that would be applicable under these provisions. We suggest that they would be a good starting point. There are, as I mentioned, the guidelines under section 8 that apply to ASIO and they too could be looked at as forming a benchmark to either go into a memorandum of understanding to apply across the board to those agencies that would be participating in the scheme. As I mentioned, there will be agencies with different types of privacy coverage and different information handling requirements. Achieving consistency, I think, would be the best outcome in this situation.

Senator BARNETT—How long is all that going to take and how important is it to ensure that the framework is in place before this legislation kicks in?

Mr Pilgrim—I am not quite sure how long it would take. That would come down to the resources allocated to doing it and who was undertaking it.

Senator BARNETT—Let us say you had the resources—are we talking weeks or months or—?

Mr Pilgrim—I would suggest you would be looking more at months than weeks to do that.

Senator BARNETT—My point is that that is unlikely to occur. They want to recommend the commencement date be the date for royal assent—that is, pretty much forthwith. So you are really suggesting that it be put on hold until those arrangements and that privacy framework is in place.

Mr Pilgrim—No, I am not suggesting that. If there is a will to put in an appropriate level of resources then, when I say 'months', it may not be three months given that we do have the basis of privacy controls within the act that already exists and that there are already sections, as I said, within section 8 of the ASIO guidelines which could be applicable. A team of people working on those could, I am sure, pull together a certain appropriate level of privacy guidance within a suitable period of time.

Senator BARNETT—That is something that we need to work through, perhaps, with the department when they appear here later on. We will check with them on that. On this other privacy issue regarding ASIO and the Australian Crime Commission: they are currently excluded from the Privacy Act, is that correct?

Mr Pilgrim—Yes, both of those organisations are not covered by the Privacy Act.

Senator BARNETT—Yes, that is right. Under the bill, its regulations can prescribe other law enforcement agencies that would likewise be excluded from the Privacy Act. Is that your understanding?

Mr Pilgrim—I would have to double-check that, but, in terms of interactions with ASIO, for example, any information that is exchanged becomes exempt from the Privacy Act.

Senator BARNETT—Yes, that is right. My point is: what is your view about, let us say, those other law enforcement agencies that are in that relationship? You do not have a problem about that? Or do you have any submission to us about what rules should apply in that case?

Mr Pilgrim—I think that comes back to the recommendations we are making about having guidelines—where they can be binding, in particular—to apply to organisations about how that data sharing can occur, what will happen with that information, how it will be handled and what uses it can be put to. That should be bound up in legally binding arrangements through memorandums of understanding, for example.

Senator BARNETT—Yes, I know. This is a bit of a tricky area, because when you are talking guidelines we are not sure—it is not legislation; it is not regulation; it is what it says it is: it is a guideline rather than some sort of legislative instrument. So I would like to know how far you want to push this guideline, whether it should be a legislative instrument of sorts or whether it should just be a guideline that will assist and help the relevant stakeholders.

Mr Pilgrim—One of the things I may like to do is give that a bit more thought and take it on notice, but there are a number of mechanisms by which guidance can be made binding. As you would be aware, it could be done through regulation itself, so a form of guidance, for example, could be developed and then could be prescribed through a regulation-making process—but that is just thinking off the top of my head in regard to that one. If you would like us to give more considered thought to that, we could.

Senator BARNETT—It would be useful for the committee, I think, if possible. The other issue I had was just as a sort of devil's advocate. The Australian Privacy Foundation are on our witness list here, and they have indicated that the bill destroys 'the hitherto carefully maintained separation between the roles of national security and law enforcement'. I hope I have not mistaken their quote there. Do you have a view about their submission and the merit of their arguments in their submission?

Mr Pilgrim—No, I do not have a particular view on that particular issue. Needless to say, there are a number of issues that need to be carefully balanced in terms of national security and law enforcement and what operations may require the sharing of information to the benefit of the community. The role of our office—and I am not trying to hide behind the act here by saying this—is that we have never had a jurisdictional responsibility or regulatory responsibility on ASIO or the other intelligence services, so formulating a comment or a position on that would be difficult, not having had a previous regulatory role and not being in a position to actually say whether the proportionality test, for example, has been met between the bill's aims and the outcomes that are desired.

Senator BARNETT—The other thing is from a business and a commercial perspective. What about the protection of confidentiality and commercial-in-confidence? Do you have a view as to how that can best be protected under these arrangements?

Mr Pilgrim—No, I do not have a particular comment on commercial confidentiality. I think our aim is looking at the personal information side, and that is more strictly our remit in this circumstance.

Senator BARNETT—Okay, thank you.

CHAIR—Mr Pilgrim, one of your key recommendations is:

Using the former Office of the Privacy Commissioner's … 4A framework to assist in ensuring the proposed amendments contained in the Bill only apply in circumstances where it is necessary and proportionate …

What is the link then between that framework and that accountability that you are looking for, and who would use that framework?

Mr Pilgrim—We think the framework is applicable in a number of circumstances. It could be a department in putting up a new policy proposal, to consider those issues as high-level questions to ask as they are starting to develop the policy outcome. It could be also—if I may be so bold as to say—that the parliament may want to look at it as well and use that framework to say, 'Do you believe that the proportionality test is being met here between what is aimed to be addressed and the methods being used?'

The accountability side then comes to the point where, once a decision has been made to move ahead, we ask: what are going to be the accountability measures down the track to test that these provisions are actually achieving what they said they were going to achieve; and what are the monitoring mechanisms that sit with them to ensure that during their life there is a process by which there is transparency about how they are being used?

CHAIR—And are you suggesting at this point in time that you are not convinced there are enough checks and balances in this—or are they yet to be developed?

Mr Pilgrim—No, we have not said that. But what we try to do is put forward a model by which, as I said, departments or the parliament can start trying to weigh up the arguments that are before them in terms of a set of amendments such as this. What we have done through our submission is look at, I suppose, the nuts and bolts of the transfer of the information and how it is proposed to be used and try to put forward ways in which we think the existing provisions can be enhanced to make them more privacy sensitive.

CHAIR—The 4A framework is not in your submission, though.

Mr Pilgrim—It was attachment A to our submission, I believe. If it is not, I can certainly provide you with another copy.

CHAIR—You are right; it is.

Mr Pilgrim—Again, as I said, Senator, it is a higher-level framework.

CHAIR—Yes, I see. The other thing I wanted to ask you about was the explanatory memorandum. You purport that it is deficient in that it needs to be revised to 'expressly canvass where privacy issues may arise within the context of these proposed amendments'. So it needs a revision? When it comes into the Senate for debate, are you suggesting that the minister responsible table a revised explanatory memorandum?

Mr Pilgrim—Whether you call it a revision or it is revised, we have certainly suggested that there are some areas which we think could benefit from further explanation in terms of some of the privacy issues around consent—just to expand on them so that they are clearer to the organisations and agencies that are going to actually be using the provisions, to get a better understanding of the intent. We have been, I think, quite explicit in a couple of areas within the submission about where we think the explanatory memorandum could be beefed up a bit.

CHAIR—Okay. That is all I had. Senator Barnett.

Senator BARNETT—We have received a supplementary submission from the Australian Privacy Foundation. I am not sure if you have seen it.

Mr Pilgrim—I saw it very briefly this morning when I travelled in.

Senator BARNETT—No problem. They have indicated, and it is now on the public record, that they were 'disappointed' by your submission. It is a free country; they are entitled to express those views. But I was wondering if you had any response to their concerns. They say:

… the OAIC is failing to adequately perform its statutory functions—specifically Privacy Act 1988 s.27(1)(b), (f) and (r).

Do you have a comment in response to that?

Mr Pilgrim—As you said, Senator, it is a free country and they are entitled to have their opinion on how we as an organisation and I as the Privacy Commissioner undertake our statutory functions. We have a statutory responsibility, which is to provide comment on bills and enactments, and we have done that, and I

would suggest we have done that in an area where we do not have an actual formal regulatory role over several of the key agencies involved or in the Telecommunications (Interception and Access) Act. So our purpose in putting in a submission was to address those areas within the provisions where we thought some enhancements could be made to the handling of personal information, and I think that that is incumbent upon me as Privacy Commissioner and upon the office, in accordance with the Privacy Act provisions that you have quoted.

Senator BARNETT—All right. They also state that they believe their views are supported by the Queensland CCL, the New South Wales CCL, the Law Council of Australia and the Castan Centre for Human Rights Law. If there is anything further you wish to share with us on notice in response to their concerns, we would welcome it. We look forward to hearing from you in due course. Thank you again.

Mr Pilgrim—Thank you, Senator.

CHAIR—Mr Pilgrim, thank you very much. Thanks for your submission and thanks for your time today. It is much appreciated.

[2.49 pm]

CLARKE, Dr Roger, Chair, Australian Privacy Foundation

CHAIR—I now welcome the Chair of the Australian Privacy Foundation. We have a submission from the Australian Privacy Foundation which we have designated as submission No. 9 for our purposes. Dr Clarke, good afternoon. Before I ask you to make an opening statement, do you need to make any changes to that submission?

Dr Clarke—No, thank you.

CHAIR—Let us have your opening statement and we will go to questions when you have finished.

Dr Clarke—I draw to your attention the context in which this bill has been tabled. Since 2001, massive constraints on civil liberties have been enacted by the parliament in over 40 statutes, comprising many scores of provisions, which lack justification or controls and which have yet to be revisited by the parliament despite undertakings given to do so. The current bill would take that assault on democracy even further.

The bill has been tabled with no prior consultation with civil society on the matter. As far as I can interpolate, it has been undertaken with no prior consultation with the Privacy Commissioner, because the submission that he provided made no reference to it and appeared to contain quite basic discussion items that he would have taken up with the sponsors had they consulted with him previously. The bill has been tabled with no prior consultation with industry, despite what the Communications Alliance had understood to be an undertaking by the sponsors to do so. Added to that, it is an omnibus bill which contains many items that are not closely related, where each of those items is the subject of complex amendments to complex provisions.

All of the five civil society organisations that submitted to the inquiry have encountered considerable difficulty in working out what the bill is actually doing. Legislative drafting, particularly in matters relating to national security, has become an exercise in obfuscation, not openness. The explanatory memorandum and the Attorney-General's subsequent submission failed to clearly convey the nature, let alone the gravity, of the bill's impacts, and the sponsoring agencies have continued the much criticised practice of failing to provide a revision marked version of the current statutes to assist in analysis of the bill's meanings and effects.

As previously quoted—thank you, Senator Barnett—the heart of the matter is that the bill's effect is to destroy the hitherto carefully maintained separation between the roles of national security and law enforcement. That is to be achieved by this bill through a complex pattern of amendments in schedule 6, involving a number of amended and new clauses. Our submission points to many of them. The Castan Centre and the Law Council submissions point to those and more. The impact of this is such a gross attack on a vital plank of democratic freedoms that the most extraordinary and substantial justifications would have to exist before the parliament should ever contemplate such measures. Far from demonstrating such needs, the bill's sponsors have once again merely asserted need and expect the public and the parliament to accept that assertion.

Submission 13 from the Privacy Commissioner has already been discussed, in the previous session. Notwithstanding Mr Pilgrim's comments just now, he has not read and taken account of the broadness of the particular powers that we referred to in our submission. He has either pretended or erred in thinking that those powers are constrained by the particular extent of powers he has in relation to regulation. They are not so constrained. He has the authority and responsibility under that section of his act to do far more than merely suggest tinkering at the edges. He has an obligation to apply, for example, his 4A framework and to draw conclusions relating to such things as the proportionality of the measures. He has failed to do so.

The particular concern that we have arising from that witness is that this committee and the parliament as a whole could be forgiven for thinking that the OAIC has actually endorsed this bill. We submit that such an inference is unwarranted, because the Privacy Commissioner's analysis has been superficial and uncritical. As you have noted, our submission and supplementary submission addressed that, and our supplementary submission is supported by QCCL and the New South Wales Council for Civil Liberties.

Where a bill contains such extreme measures and demands such effort from civil society to unmask them, there is a natural tendency to focus on the extreme measures alone. As a result, the many other provisions in the other six schedules have tended to be short changed by the civil society organisations that have considered the bill. We therefore submit that it is not adequate to merely amend the bill through deletion of schedule 6.

In summary, the separation of national security functions from mainstream law enforcement is vitally important, as is assurance that the extraordinary powers granted to the small number of national security agencies do not become either directly or indirectly available to any other agencies for any other purposes. As noted, our original submission has been endorsed by QCCL, and the concerns in it have been separately voiced by the New South Wales Council for Civil Liberties, the Law Council of Australia and the Castan Centre for Human Rights Law—the last two of which we did not have any contact with prior to our submission going in.

The APF accordingly urges the committee to do everything in its power to ensure that the bill does not proceed. We submit that the bill's sponsor should be advised to remove all of the provisions that would destroy the carefully prepared barriers between national security and law enforcement functions, that they should be advised to prepare a list of existing definitions relating to national security and law enforcement functions and the ambiguities and overlaps among those definitions and, to go with that, a list of possible new definitions of key terms. They should further prepare justification for each of the amendments for which parliament's approval is to be sought, and they should provide a revision-marked version of the acts as they would appear if the bills were passed. They should further be advised that the expectation of Senate committees is that sponsors of bills consult, prior to submission to the parliament, with civil society, affected industry and the Privacy Commissioner and then adapt the proposal in the bill to reflect the concerns that have been expressed. We also believe that they should be submitting to the parliament separate bills whose impacts are clear and that also do not warrant the very substantial criticisms that have had to be made before this committee by civil society organisations. Thank you.

CHAIR—Thank you. I do not know where to start, really. There are such major criticisms and specific comments on a range of items in the bill. Can you outline for me why you believe the bill conflates the significant distinctions between national security, national intelligence and criminal law enforcement? Why do you believe it does that?

Dr Clarke—Hitherto, national security legislation has related specifically to national security and it has generally been fairly clear what the delineated agencies have been that have been empowered and given extraordinary and, as we said, insufficiently justified and insufficiently controlled powers. What this does, through several different mechanisms which are difficult to disentangle, is enable information to flow and functions to be performed across boundaries to law enforcement agencies which have not previously had these kinds of involvements, these kinds of powers or these kinds of information flows. We are talking here about extraordinarily privileged information gathered by national security agencies under extraordinary powers, and playing those, with all of the enormous uncertainties and lack of controls that they involve, into the many different conventional law enforcement contexts is unjust and inappropriate.

CHAIR—So it is broadening the range of agencies as well as their powers.

Dr Clarke—Yes.

CHAIR—You do not believe that the range of agencies should be broadened?

Dr Clarke—The parliament has seen fit to approve this legislation against our prior submissions and the submissions of the entire nation's lawyers. Under no circumstances should the powers that have been granted to national security agencies be allowed to extend out to law enforcement agencies generally. That is the effect of this bill.

CHAIR—You believe there should be a clear delineation in the actual statute?

Dr Clarke—A clear delineation. It is not as clear as it might be; hence the suggestion that the definitions need to be re-examined and studied. But hitherto, to an extent, there has at least been some quarantining of these extraordinary powers into the national security community alone.

CHAIR—Have you given any thought to the criticisms that were raised by the Communications Alliance about the impact this has on providers, or have you stayed more with your focus on the impact this has on people's rights and civil liberties?

Dr Clarke—In my personal role I am an e-business consultant. I have some knowledge of those areas and some association with some of those industry associations, and I am sympathetic to their views. The Privacy Foundation has had to focus specifically on the aspects that we could see had a major privacy impact; therefore, we have not looked at the difficulties for telcos.

CHAIR—There were some concerns expressed by the information commissioner about the explanatory memorandum needing to be more clear about what is intended. You have gone a bit further. You have identified four paragraphs where you think there needs to be better and further particulars or definitions. So you believe there are quite a number of areas in the explanatory memorandum that need revising and retabling in order to make the bill clearer?

Dr Clarke—It would have been helpful to us if that had been done prior to consultation, or even prior to our consideration of the documents before the parliament. It does not alter the fact that—how can I put this politely—we can read through the misleading information that is contained in the explanatory memorandum to appreciate what the real effect of the bill is; and, because of that real effect, we submit to you that the explanatory memorandum should disappear out the door of the parliament in the same way that the bill should.

Senator BARNETT—The chair has touched on most of the key points. Your views are very soundly expressed in your submission and in your opening statement, but can I just go back to the fundamental crux of this—that is, the foundation's view with respect to the right of the government to expand the law enforcement agencies covered by this bill. That would include not just the Australian Crime Commission and ASIO but other law enforcement agencies. Do you have a fundamental problem with the extension of the powers to those agencies, or is the problem the matter in which those powers are extended and the lack of safeguards surrounding that extension?

Dr Clarke—The parliament, as distinct from the government, clearly has the power to do that which the parliament sees fit to do. We strenuously argued five years ago, possibly in this same room, against the last tranche of massive depredations that went through—and that was supported by both sides of the House, as I recall. What they did was to separate—perhaps 'sequester' is too strong a word—into definable national security agencies those extraordinary, unjustified, uncontrolled powers. It is absolutely essential that parliament not sleepwalk its way into permitting those kinds of extraordinary powers to leak across the boundaries. In a free society the distinctions between national security agencies and functions and law enforcement agencies and functions must be sustained. So, we do not see this as being capable of any kind of bandaid approach.

Senator BARNETT—So, really, your fundamental concern, as you indicated in your opening remarks, is the need for a comprehensive review of our security and law enforcement powers that were implemented is some four or five years ago?

Dr Clarke—Absolutely.

Senator BARNETT—And you are saying that that has not occurred and it needs to happen?

Dr Clarke—Correct.

CHAIR—Dr Clarke, I am going to ask you a question which may be totally unrelated to this. I think it does relate to the telecommunications interception bill, and may well come before this committee if ever we get the journalists' shield legislation. It is probably not directly related to this at all—although it may well be. It is a matter you may well have followed with interest that has blown up in the Northern Territory in the last three or four days, where—and I am not sure if you have been following the story—the Northern Territory Police have seized the mobile communications records of a journalist in the Northern Territory in order to source his leak for a story he ran. These records were seized without his knowledge.

It has been put to us up there that, as to the journalists' shield laws that are now coming before this parliament, unless there is a change to the Telecommunications (Interception) Act, there will be a backdoor means by which you can seize information from journalists unless this loophole is closed.

In a funny, roundabout way, it is related to this act, in this provision now. It is the same act. It would be interesting to know, if this bill grants more agencies an expanded role, whether that implicates them in any of that behaviour and whether or not that is a loophole in the telecommunications act, with regard to sources of information that journalists receive via telephone, that this committee would need to look at. I will leave you with that as a question on notice to ponder. You might want to have a look at the stories that have been running in the *Northern Territory News* and on ABC radio in the last four days up there.

Dr Clarke—I would like to make a couple of quick comments giving my reactions to that, because it is an extremely interesting matter, which I had not been aware of because I have been travelling in the last several days.

CHAIR—That is as I thought.

Dr Clarke—Firstly, it is a legal question. Secondly, it is an extraordinarily complex legal question which, I suspect, the best brains in the country would have trouble unravelling right now—that is to say, marking up the existing legislation with the changes that the bill would envisage and then trying to work through all the implications of that. Thirdly, it is entirely credible, on our reading of this, that the loophole could exist that could enable such extension. But the reason I say that is: this schedule 6 is designed as a mass loophole creator. It is intended to enable leakage of significant powers across into agencies and functions of a law enforcement nature. The implications of that could be far and wide, and journalists' shield matters would be just one of the potential areas of collateral damage that could occur.

CHAIR—It has been put by Ken Parish, a lecturer at Charles Darwin University, in the last 48 hours that there is no point in having a journalists' shield bill unless you can close this loophole in the Telecommunications (Interception) Act. Otherwise you could, through the back door, through powers that police—in this case, the Northern Territory Police—have, seize the telecommunications records of a journalist, without his knowledge, to ascertain the source of the story he ran.

Dr Clarke—I would regard Professor Parish as being far more likely to be able to provide accurate advice on this specific matter than I or my other, voluntary colleagues—lawyers though many of them are—would be. I would think he would be an appropriate source of analyses of that kind. My position has to be that I would be surprised and extremely disappointed if the existing law provided such a loophole. Clearly the Northern Territory Police believe they have got one. I would be totally unsurprised if this new schedule 6 did not open up such loopholes.

CHAIR—You might perhaps, with your colleagues, have a look at that scenario and get back to us then.

Dr Clarke—If we are able to come up with anything useful for you—

CHAIR—It is not a scenario; it is a story of fact.

Dr Clarke—Yes. If we are able to come up with any useful analysis for you, we will do so.

CHAIR—Thank you very much for your submission and thanks for your time today.

Proceedings suspended from 2.50 pm to 3.04 pm

DONOVAN, Ms Helen, Co-Director, Criminal Law and Human Rights, Law Council of Australia

Evidence was taken via teleconference—

CHAIR—Welcome to our public hearing, Ms Donovan. We have a submission from the Law Council which we have designated No. 4. Do you need to make any changes or alterations to that submission?

Ms Donovan—No.

CHAIR—I invite you to make some opening comments and then we will go to questions.

Ms Donovan—Firstly, I thank the committee for the opportunity to appear today on behalf of the Law Council. I should note that I was to appear today with Mr Phillip Boulton SC but, as a result of the schedule change, Mr Boulton is now tied up in court and unable to appear. I will attempt to field senators' questions myself but I may have to take them on notice.

The bill introduces a range of amendments but the Law Council is primarily concerned with two proposed areas of reform. The first is schedule 6, item 12, which allows ASIO to share information with a wider range of agencies about a wider range of matters. The second is schedule 6, items 11 and 17, which allow for ASIO personnel and resources to be used by other agencies, including for purposes unrelated to ASIO's existing functions.

On the first matter, which relates to increased information sharing, the Law Council acknowledges that it is important that the safety and security of the nation are not jeopardised because government agencies are unable to share information in a way which allows credible national security threats to be promptly and effectively identified and neutralised. There has been much written and said recently about the need for greater cooperation and information sharing between agencies, but the barriers appear to be more about different organisational cultures and practices than about genuine legislative obstacles to cooperation.

The ASIO Act already allows for information sharing with law enforcement agencies where ASIO has information which relates to, or even just appears to relate to, the commission or intended commission of an offence. The existing provision is already a reasonably permissive provision, and the examples which have been given to explain why information sharing is necessary and desirable—such as the prevention of an aircraft bombing—would appear to be already adequately catered for by this provision. The question therefore is: what type of information is currently contained in ASIO's information silo that cannot be shared but should be or needs to be? A few examples would be illuminating.

As it stands, it raises alarm bells when it is proposed that ASIO should be able to share information whenever ASIO deems that it is in the national interest to do so—whatever that nebulous term means. One thing is for certain: we can be sure that it is a reasonably broad term. As Phillip Boulton, on reviewing the legislation, has pointed out, the understanding of 'information that relates to national security' in the national security information act is quite broad, and 'information that relates to the national interest' must be broader than that.

It is worth emphasising that the reason these provisions raise alarm bells is not just that information sharing in itself introduces privacy concerns. The issue is also that ASIO has a range of extraordinary and covert powers which are intended to be utilised for very specific and serious purposes, and allowing information obtained through the use of those powers to be shared with few restrictions increases the risk that ASIO's powers will be used for improper or collateral purposes. That is the issue at the heart of the Law Council's concerns.

On the second issue, which relates to the use of ASIO personnel and resources by other agencies, again the Law Council acknowledges the need for cooperation between agencies. But, again, the current provision is already reasonably permissive. ASIO is currently authorised to cooperate with other Commonwealth, state and foreign government agencies, provided that such cooperation is necessary for, or even just conducive to, the performance of ASIO functions. The Law Council's view would be that the legislation should facilitate cooperation between agencies where their functions converge, but not otherwise. As the Law Council has pointed out in its submission, the safeguards which are in place to ensure that ASIO personnel operate within a lawful framework are dependent on a clear articulation of ASIO's functions. Those safeguards would be undermined to some extent by a provision which allows ASIO personnel to pursue unrelated functions for other agencies.

In closing, I simply note that in its submission the Law Council has raised a number of questions about the intended operation of amendments proposed by the bill. At the very least, our hope is that the legislation is not passed until the types of issues raised by those questions are fully and publicly ventilated. Our view is that they have not been to date.

CHAIR—Thank you, Ms Donovan. I might start with a question to you. Can you envisage a situation where ASIO would actually need to share information with a wider range of government agencies other than law enforcement agencies?

Ms Donovan—No. There is possibly one—in fact, there may be well be one—but that is the sort of question that we would like to see directed at the agencies and departments so that we have a better understanding about what this bill is intended to achieve. It is interesting, because the explanatory memorandum says that the reason for expanding the group of agencies with whom ASIO can share information is that by having an exhaustive list in the legislation there is a risk that a new agency will be created or an existing agency will be given new functions and the exhaustive list will no longer be adequate. Our view would be that if a new agency is created or an existing agency is given different or expanded functions then the legislation which achieves that end, which creates the agency or expands its functions, should also if necessary amend the ASIO Act. The legislation should be preceded by a consideration of whether that new agency ought to be one with whom ASIO can share information. Our view would be that that is not overly cumbersome.

CHAIR—So you are not aware of any case law or issues that have arisen in the last year or two years that point to a need to amend the Telecommunications (Interception and Access) Act.

Ms Donovan—I am speaking about amendments to the ASIO Act rather than to the telecommunications interception act.

CHAIR—My question, though, is: are you aware of any instances where court rulings or court suggestions or barriers have suggested that this amendment to the ASIO Act is needed?

Ms Donovan—I am not aware of any.

CHAIR—Is there a suggestion, perhaps, that information coming into ASIO's possession outside Australia or matters outside Australia would broaden the need to give information to an agency that is not a law enforcement agency—such as DFAT, for example?

Ms Donovan—There is already provision under the ASIO Act for information which is obtained outside Australia to be shared with a minister or a department where it is deemed by the Director-General to be in the national interest.

CHAIR—What is your understanding of what the national interest is?

Ms Donovan—As far as I understand it, that provision is not defined in the act at present. Our concern is that, at present, information which does not relate to the commission of an offence or the intended commission of an offence but only relates to the national interest can only be shared where that information is obtained overseas or relates to activities overseas. It is now proposed that information may be shared even if it is obtained in Australia and relates to events within Australia, as long as it is in the national interest, even where it does not relate to the commission of an offence. As far as I am aware, the term 'national interest' is not defined in the ASIO Act. It is used in other contexts, but no doubt the representatives from ASIO will be able to give you information about how they understand that term. As I mentioned in my opening statement, the national security information act, which governs, for example, proceedings in antiterror trials, talks about information which relates to national security, and that has been understood very broadly to concern matters relevant to Australia's political and economic interests and interactions with foreign governments and organisations.

CHAIR—Have you had a chance to look at the Information Commissioner's or the Privacy Foundation's submissions to us? Both of them have criticisms in there of aspects of the explanatory memorandum.

Ms Donovan—Yes, I have had an opportunity to read both of them.

CHAIR—Do you want to make a comment about whether the Law Council believes their criticism about the inadequacies of the memorandum is fair or unfair?

Ms Donovan—I think that the criticisms are fair, because the explanatory memorandum does not adequately address what the existing legislation already provides and allows for and does not provide adequate explanation as to why those existing provisions do not meet the needs of the agencies and the nation at present.

The examples which are given to justify some of the amendments are already appropriately addressed by existing provisions. As our submission starts, as an outsider to this process it is very difficult to comprehend what sort of problems this amendment act is designed to overcome and what its intended practical effect is. The reason our submission is framed as a series of questions is that, in looking at the legislation and attempting to analyse and understand it, we are left wondering.

CHAIR—Thank you.

Senator BARNETT—Having read your submission in which you have asked all those questions, I will be quite honest with you that I do not have the answers. But we are going to have the department here shortly, so no doubt we will take the opportunity to put those questions to the departmental representatives and see if we can get some answers. I am particularly interested in your concerns regarding schedule 6 and items 12 and 17, as outlined in your opening remarks and, prima facie, they seem to be compelling arguments. How serious are your concerns? Are they serious enough to suggest that the Law Council would not wish the bill to proceed until the arguments that are put in the bill are justified by the department? How strongly do you feel about these concerns?

Ms Donovan—Our position is that the bill should not be passed—that those items of the bill, at least, should not be passed—until adequate explanation is provided as to why they are necessary and how they are intended to be used. In addition to that, having read the submission of the Information Commissioner, if the provisions are going to be passed then there are certainly additional regulations and safeguards which need to be put in place.

Senator BARNETT—The Privacy Commissioner was here earlier and indicated a privacy framework or some sort of guidelines that should be put in place, and whether they should be regulatory or some sort of legislative instrument in nature or more of an MOU, as he referred to it, or some sort of guidelines. I think he was open to discussion on that. But there are two threshold questions based on your response just then. Firstly, you say the bill should not proceed unless there is further evidence—let us say that the department says there is evidence that ASIO does need to liaise and work with other law enforcement agencies and other key agencies—

Ms Donovan—In a way that is not currently facilitated by the legislation.

Senator BARNETT—Correct. So let us say they say that it is necessary; what are you going to say?

Ms Donovan—If a genuine need is demonstrated then I think the submission of the Information Commissioner comes into play, and what we need to consider is: if those information flows are necessary and are going to occur, how will they be regulated? How will secondary disclosure be regulated? How will information handling more generally be regulated in terms of storage, destruction, et cetera?

Senator BARNETT—So you are saying that you need to know that before you are able to respond to the committee and advise on what sort of privacy framework regime should then be implemented?

Ms Donovan—That would be my position, yes. Otherwise to assume that this information sharing should be facilitated is putting the horse before the cart to some extent.

Senator BARNETT—I can see the logic of your argument. The only issue is that we have a bill before us, and no doubt the government will want to proceed normally within the timeframe that they have allocated. So we have some issues, frankly.

Ms Donovan—I can understand that. It is unfortunate that those timeframes might dictate the extent to which the issues presented by this bill can be properly discussed and ventilated—particularly when as far as I am aware there has not been consultation, particularly on these provisions, with people outside the agencies prior to the introduction of the bill to parliament.

Senator BARNETT—That is what I was about to ask you about—the level of consultation, if any, regarding the bill.

Ms Donovan—As far as I am aware, there was no consultation on the provisions that our submission is directed towards.

Senator BARNETT—Right. What about the thrust or the substance of the bill more generally? Was there any consultation?

Ms Donovan—Not as far as I am aware. I know that some of the other issues that are addressed by the bill—the missing person provisions and the victims of crime provisions—were discussed more generally in the

context of the ALRC review. And to some extent the issues that I am raising were discussed in the context of the ALRC review. But not these specific provisions.

Senator BARNETT—I want to clarify: the Australian Law Reform Commission review?

Ms Donovan—Its general review into privacy touched on information sharing between intelligence agencies and law enforcement agencies. As the submission of the Information Commissioner points out, a number of recommendations were made about the need for greater regulation of information flows, particularly between agencies that are not subject to the Privacy Act and other agencies.

Senator BARNETT—Do you recall when that discussion took place?

Ms Donovan—The final report is at least 12 months old and the review preceded that. But it was looking at the framework that was already in place under the ASIO Act. The ALRC took the view, for example, that greater direction and regulation was required. It was not looking at these specific provisions and the possibility for increased information sharing.

Senator BARNETT—All right. Do you have views on the proposed definition of 'law enforcement agency'?

Ms Donovan—No, I do not have a view on that. I saw that it arose in the Privacy Foundation's submission. I agree with the general thrust of their submission: that there is a need for greater uniformity across Commonwealth legislation in how that term is used. But I do not have any submission to make about how it is defined in this particular bill.

Senator BARNETT—The supplementary question is: do you have a view on the functions of law enforcement agencies? Clearly, those functions would be broadened significantly, depending on your answer to the first question.

Ms Donovan—I am sorry, Senator: I did not follow your question.

Senator BARNETT—Your answer to the question about the definition of 'law enforcement agencies' is relevant to—

Ms Donovan—the definition of what a law enforcement function is.

Senator BARNETT—Yes. The functions of law enforcement agencies are clearly going to be much broader, depending on your answer to the first question.

Ms Donovan—That ties in to what I said earlier. In many situations, the most appropriate legislative response is going to be to have an exhaustive list of agencies. I do not think it is that onerous or cumbersome to list those.

Senator BARNETT—All right. On another matter regarding schedule 3, I note that the New South Wales Police Force indicate in their submission that amendments made to schedule 3 would enhance the ability of law enforcement agencies to locate missing persons where no issues of criminality are involved. I do not know if you have perused their submission or the submission of the Australian Federal Police. Do you have any feedback on their submissions?

Ms Donovan—I have read their submissions. Is the issue you are addressing the one raised by the Information Commissioner, that this represents an expansion of the use of the Telecommunications Interception Act into areas unrelated to law enforcement?

Senator BARNETT—That is part of that, and clearly it seems to me you are concerned and the Privacy Foundation is concerned about that. Is that correct?

Ms Donovan—I can see some merit in the proposed provisions which would allow the release of telecommunications data to be authorised for this purpose. The Information Commissioner has made a number of I think very sensible recommendations about the need for further guidance to be included in the legislation or in the regulations about the secondary disclosure of that information where direct consent is not given by the missing person themselves, where it is either implied or it cannot be given due to that person being somehow incapacitated. The Law Council would certainly endorse the recommendations of the Information Commissioner in that respect.

Senator BARNETT—Finally, going back to my first question and your two main concerns, schedule 6 items 12 and 17, I think they were, based on your reading of the bill, do you think ASIO could share the information they gain with the minister?

Ms Donovan—The ASIO Act already allows information to be shared with a minister where it is in the national interest if it relates to information outside of Australia or was obtained outside of Australia. Is your concern—

Senator BARNETT—Just going to your main concern, schedule 6 items 12 and 17, and ASIO's use of information that they may gain in discussion and in liaison in relationship with other law enforcement agencies and then whether they have the ability or the legal capacity to share that information with their minister.

Ms Donovan—As I said, I think they already have some capacity to share that information with the minister at present.

Senator BARNETT—Yes, but this is going to increase that capacity, isn't it?

Ms Donovan—I do not have at hand the definition of a Commonwealth agency, but I think it does include a minister. Could I take that question on notice?

Senator BARNETT—Of course.

Ms Donovan—I will have a look at the definition and seek some advice about whether it includes a minister. I do not have it in front of me. It might be quite straightforward.

Senator BARNETT—All right. So no doubt you will be waiting with bated breath for the evidence of the department with respect to answering some of the questions you put in your submission.

Ms Donovan—I would hope there is the opportunity to discuss some of those matters with the department and the agencies, yes.

CHAIR—Ms Donovan, thank you very much for your time this afternoon, and also the submission from the Law Council is much appreciated.

Ms Donovan—Thank you for the opportunity.

[3.30 pm]

BARTON, Superintendent Brad, Coordinator, Technical Capability Delivery, High Tech Crime Operations, Australian Federal Police

FRICKER, Mr David, Deputy Director-General, Australian Security Intelligence Organisation

McDONALD, Mr Geoff Angus, Acting Deputy Secretary, National Security and Criminal Justice Group, Attorney-General's Department

MUNSIE, Ms Laura Rosina, Principal Legal Officer, Security Law Branch, Attorney-General's Department

OBEROI, Ms Sabeena, Assistant Secretary, Cyber Security and Asia-Pacific Engagement Branch, Department of Broadband, Communications and the Digital Economy

STRAUSS, Commander Jamie, Acting National Manager, High Tech Crime Operations, Australian Federal Police

WHOWELL, Mr Peter, Manager, Government Relations, Australian Federal Police

WILLING, Ms Annette Maree, Assistant Secretary, Security Law Branch, Attorney-General's Department

WINDEYER, Mr Richard James, First Assistant Secretary, Digital Economy Strategy Division, Department of Broadband, Communications and the Digital Economy

CHAIR—Welcome everybody. I remind people that the Senate has resolved that an officer of a department of the Commonwealth or of a state shall not be asked to give opinions on matters of policy and shall be given reasonable opportunity to refer questions asked of the officer to either a superior officer or the minister. This resolution prohibits only questions asking for opinions on matters of policy; it does not preclude questions asking for explanations or factual questions about when and how policies were adopted. Do you all have opening statements, or just somebody? We are feeling a bit outnumbered, I have to say.

Mr McDonald—We thank you for putting us all on at once, because it makes it a bit easier for everyone. We thank you for the opportunity for our department to appear before this committee. As you are aware, the department has made a submission about the bill to the committee. There are a couple of key points we would like to start with which refer to the National Security Statement back on 4 December 2008, which highlighted the need for a closer relationship between agencies within the national security community and the critical need for the sharing of information and data between agencies. The National Security Statement not just is about traditional national security issues of spying and terrorism but takes into account serious and organised crime and matters like that—it has a broader perspective.

I should also refer to the counterterrorism white paper, which also stressed the need for sharing of information. I think I heard earlier the statement that there were cultural barriers to break down, and certainly in my time in the space some of those have broken down considerably, which has been facilitated by the setting up of joint committees and the like within the agencies. The National Threat Assessment Centre is an example of that and the Counterterrorism Control Centre is another one. However, we have found that there are some legislative constraints in the legislation, which have been addressed in this bill. You have to be very sure about your legislation when it comes to passing on information for action which may have an impact on individuals, particularly where it involves offences. The bill is about enhancing that cooperation.

Of course, all the resources in this space are in support of the national security priorities of the government. There are very considerable resources in it. One example of such an agency is the National Threat Assessment Centre. There you have together a whole range of agencies developing threat assessments for the government so that decisions can be made about protective security. While ASIO has intelligence collection and assessment functions, other agencies involved in this have other functions. We think the bill will remove unnecessary legislative barriers to the sharing of that information. An example of how they can share and help each other is in the area of languages. As you know, we have people from all over the world in this country, from hundreds of countries, but of course within those countries there are scores of languages. Sometimes the language resource that agencies have access to is very limited, in having the right proficiency for the sort of work that these agencies do.

I should point out that the Inspector-General of Intelligence and Security provides important independent oversight in this area. If you read the latest annual report you will see that the IGIS is a fairly fearless and

frank oversight body in this space. That role is addressed in the National Security Legislation Amendment Bill 2010, which is also before the parliament, where the ability of the IGIS is extended.

The amendments to the interception act are very focused on much the same thing in terms of assistance cooperation between ASIO and law enforcement, ensuring that there is improved technical capacity with law enforcement. We have amendments such as those to do with the finding of missing persons and solving crimes where the victim cannot be found and cannot consent to communications being accessed. Again, this is to clarify the law so that we do not have a situation where we go too far in restricting coverage.

I point out that we have a lot of reporting requirements. All those are in place. I also point out that we have a quite sophisticated relationship when interacting with industry in terms of access to telecommunications interception. I will let you get on with your questions.

CHAIR—Mr McDonald, were you reading from your submission or were they additional opening remarks?

Mr McDonald—These are just our notes.

CHAIR—Can you give me an example of where agencies may well need to share information outside law enforcement agencies? Give me an example of an agency and what sort of information would need to be shared.

Mr McDonald—Straight up, I will give you three examples. At the moment it is essentially about getting information very quickly. Nowadays, with the way things are with communications and transport, things happen extremely quickly. One example is the ability to pass information on to the people who administer the Migration Act. Another example might be the Taxation Office, where ASIO comes across an absolutely huge taxation fraud which would affect government revenue and your ability to look after the community by reducing revenue—the Project Wickenby task force is an example. It is quite possible for an agency like ASIO as part of its normal functions to come across something relevant to that. As we know, people that ASIO might be interested in under its normal functions are sometimes involved in other illegal activities.

I have been listening to some of the committee's deliberations. A really important consideration is the police integrity and anticorruption bodies. ASIO is involved in covert work, and, if there was ever an area where stuff is done covertly, it is in the context of corruption. The chance of ASIO coming across corrupt activity is quite high. It could be corrupt police activity, in which case the appropriate place to send that would be to the integrity commission. So there is quite a bit in just those three examples.

I think I heard a suggestion that every time we have a name change for an organisation or the like we should come back with an act of parliament or a different organisation. As you know, the legislative program is very busy and it takes some time to do that. Sometimes you may have an emergency situation where listing the correct organisation quickly might well impact on things operationally. Of course, the parliament can disallow the regulations which provide the listings.

CHAIR—You would have heard the Law Council's evidence, which suggested that the changes regarding the amendments to the ASIO Act in fact were not so much unnecessary but rather covered by provisions already in the act. Would someone provide me with a response to that.

Mr McDonald—I do not think that is right. I have already outlined some examples where you would not be able to pass information on just like that. I am sorry, but I respectfully disagree. We would not be going through this—

CHAIR—You are saying the changes in this legislation need to ensure that the flow of that information is done under a regulatory framework that, if it needed to be tested in a court of law, would be protected in that way?

Mr McDonald—Yes, that is right. The courts are absolutely meticulous about this. That is their right, but there is nothing sadder and more soul destroying than seeing guilty people go free because of a technical argument.

Senator BARNETT—Let us pursue that a little further. The Law Council of Australia specifically nominated schedule 6 items 12 and 17, as I understand it—I have the bill and their submission in front of me. Item 17 deals with 'cooperation with intelligence and law enforcement agencies in connection with performance of their functions' and item 12 covers 'communicating information to appropriate authorities of the Commonwealth or a state'. Have you read the Law Council's submission?

Mr McDonald—Yes.

Senator BARNETT—And you may have heard their evidence. So what do you say to them? Their submissions are normally very comprehensive—and this one is reasonably comprehensive, but they have put it in terms of questions because they do not understand why you need that power and how it would be implemented. The Privacy Commissioner, in his response, indicated that if that was going to be implemented there would need to be a privacy framework put in place. That was his view. I just want to work through those issues with you.

Mr McDonald—There is already a privacy framework. There are privacy guidelines which are publicly available. Those guidelines are regularly reviewed. We have a new round of privacy reforms occurring and which are in the process of being put in place. My colleague here can read you some extracts from those guidelines. You will find out that ASIO, and all the agencies, actually have quite extensive privacy guidelines and they are held to account under those by the Inspector-General of Intelligence And Security.

Senator BARNETT—Why would the Privacy Commissioner be recommending a new privacy framework to this committee if, as you are saying, a framework is already in place? Why do you think he is doing that?

Mr McDonald—What I said was that we already have a framework in place. I was not here to hear the Privacy Commissioner, but I think what the Privacy Commissioner is suggesting is that there may need to be adjustments to those guidelines to take into account the operation of these provisions. What I am saying is that that will certainly occur. Those guidelines will be reviewed in light of other changes in the privacy area that are occurring. When they say 'a new framework' it sounds like there are no guidelines at all and we need a completely separate set of guidelines. I am saying that we have guidelines that are quite good, but they will need to be reviewed in light of this legislation but possibly even more so in light of other changes to privacy legislation which are in the pipeline. Annette might be able to add something.

Ms Willing—The only other thing I would add is that the privacy considerations were taken into account in the development of this legislation. As Mr McDonald said, there is already that framework in place. The Attorney-General has issued guidelines to ASIO which are publicly available. They do include guidance as to how ASIO should performance work and include things like undertaking inquiries using as little intrusion into individual privacy as is possible and using the least intrusive techniques of information collection before more intrusive things. And there is a section about handling personal information which was developed in consultation with the Privacy Commissioner at the time and is based on the privacy principles. The other intelligence agencies also have their own privacy rules. But, again, as has just been said, we are certainly happy to look at these in light of other broader reforms that are going on in the privacy area. I understand the privacy principles are currently undergoing a Senate committee process as well. Anything we hear about those broader reforms we will take into account.

Mr McDonald—And, of course, those guidelines were put out under section 8A of the ASIO Act, which means that my colleagues here from ASIO and other people in ASIO are bound by them under the authority of the Director-General.

Ms Willing—The other thing I would add to that is that the Inspector-General is charged with looking at not only the legality but also the propriety of what ASIO does. Even if technically they can do things, there are these guidelines that govern what they should be doing. The Inspector-General looks very closely at that as well.

Senator BARNETT—The Privacy Commissioner talked about the option of having guidelines which were subsequently a legislative instrument of sorts or a memorandum of understanding which were more guidelines than a legislative instrument. Do you have a view on that?

Mr McDonald—As I said a minute ago, these are under a statute. They are under section 8A of ASIO Act. They are an instrument under legislation.

Ms Willing—Under the legislation, the minister is also required to table those in parliament as well.

Senator BARNETT—So they are required to be tabled in parliament?

Mr McDonald—Yes, they are.

Senator BARNETT—In your view, you should consult with these key stakeholders and update them as appropriate? Is that your plan? How long will that take?

Mr McDonald—First of all, this is what I expect will be the case and that would be something we would be recommending. The timing of it I would have to take on notice. I have not really assessed how long it would take. One of the things that makes it hard for me to assess that are the other elements of the privacy

changes that are occurring. It is a little hard for me to give you a specific time frame, but I will say it is something we would do as soon as practicable.

Senator BARNETT—If you are happy to take that on notice and give us a better indication that would be useful.

Mr McDonald—Yes. I started to realise how hard it would be for me to give you a specific date.

Senator BARNETT—I will leave that in your hands. The Law Council have asked a lot of questions which go back to the initial question that we put to the other witnesses about consultation. We were somewhat surprised that from their point of view there has been adequate consultation. How do you respond to that?

Mr McDonald—I think the bill was introduced some time in June. So it has been out there for quite a long time. It is not as if people have not had an opportunity to digest what was in it. It is the case that we often do much more comprehensive consultation processes. An example of that is that national security legislation and our purple discussion paper. That is for much more comprehensive and substantial changes. Sometimes with amendments like these which in our mind are not of the same nature, we do not have a particularly ornate process. That is our answer on that.

Senator BARNETT—You have consulted on most of your other bills that I can remember. I might be wrong.

Mr McDonald—You will find that there have been, although I hate to admit it, quite a few machinery bills over the years, particularly in the TI area where we have had to move reasonably quickly.

Senator BARNETT—What is the imperative in this case to move quickly?

Mr McDonald—During the budget process you might remember we had renewal of funding in the TI area. As part of that, we found a way of looking after future technological challenges by establishing a process whereby ASIO would be able to provide assistance on a pilot basis to two law enforcement agencies—the Crime Commission and ACLEI, the anticorruption body. That was part and parcel of our budget strategy. We felt that without these cooperative amendments in the TI area, we would not be able to use that pilot to its full potential. It is very important because if that pilot works, it will be quite relevant to the financing of the some of the challenges in TI. The budget figure for TI over the four years is $100 million. That is between law enforcement and—

Senator BARNETT—Are you saying that, just because the money is there, you want to get on and use it?

Mr McDonald—It is not because the money is there so much as that we have only two years to do the pilot. So it is important and—

Senator BARNETT—And you need this bill passed to do the pilot?

Mr McDonald—We can do some aspects of it but, to do the pilot in the way the whole thing is intended, yes. That was one thing that was pushing it. The second thing was that there was some concern about the plot in the US—I think it was on Christmas Eve last year. There was some criticism—I am not going to pass judgment on whether it was valid or not—of how agencies were passing information to each other in that context in the United States. We had already identified some of these legislative problems that we have got here and we were concerned that we did not want to leave open potential barriers in that context.

Senator BARNETT—Mr McDonald and others, if you want to provide on notice further particulars regarding the imperative in terms of timing, that would be appreciated.

Mr McDonald—Yes. Of course, we tried to get it through before—

Senator BARNETT—Yes, I am aware of that. Now, we have to address this issue of the telecommunications industry, the Communications Alliance Ltd. They wanted to delete schedule 2. They cannot see the need for it.

CHAIR—They want to defer it, don't they?

Senator BARNETT—Or defer it at least and come up with a mutually agreeable alternative. They are my words, not theirs. I think they indicated their willingness to work with the relevant department and agencies. What do you say to them? They indicate the additional cost, red tape and burden et cetera. It is all in their submission and their evidence. Can you provide a response?

CHAIR—Mr Windeyer, do you have any response to that in any communications you have had with the Communications Alliance?

Mr McDonald—I have got a view.

CHAIR—Yes?

Mr McDonald—I might just point out that this used to be in the legislation in 2007, and it was taken out then. It was taken out then on the basis that we thought at the time that it was so likely that people would comply with it that it was not necessary to have it in the legislation. We thought that people would provide this information because it is a very limited burden on them. It is not just us that thought it was a limited burden; the Office of Best Practice Regulation agreed with us that it was a very limited burden. But the industry had this requirement right up to 2007. Unfortunately when we did the amendments in 2007 we thought it was surplus. We have since found that there have been incidents where the industry has just had not identified that they have got a problem with their new technology. Then we have a terrible situation in terms of retrofitting it to make sure they do comply, to make sure that they have got the right technical solutions for interception, and it ends up costing them more. This is a measure which will just require them to write a letter or just advise us: 'We're moving to this technology. This is what we're planning to do.' Our friends in Asia, and of course our department as well, have quite a connection with the international networks and with other aspects of industry. Quite often if they say: 'We are interested in this technology,' we will be able to advise them, 'If you are thinking about that, understand that there are these issues you need to look into with that particular technology.' So all they have got to do is give us a letter and outline what some of their plans are. It is not burdensome.

Senator BARNETT—They say it is.

Mr McDonald—They are wrong, wrong, wrong.

Senator BARNETT—There is a 30-day time period. What do you say about the 30-day time period?

Mr McDonald—I think they must be thinking that we are expected them to provide a whole prospectus or something like that. We are just talking about the most general description about what their proposals are. It is there to help them.

CHAIR—Does the bill need to be amended to clarify that?

Mr McDonald—We are criticised all time for putting verbiage in bills. I do not think it does. If the committee was disposed to recommend something then that would be okay, but it looks pretty straightforward to me.

Senator BARNETT—What happens in that 30-day period? They are obligated to provide it to you. Is there an impediment for them to proceed unless they get your consent or agreement or acknowledgement?

Mr McDonald—They are asked to provide this in a timely manner under the act as part of their industry obligations. So they are obliged if they want to participate in this industry to provide the sort of assistance. Obviously we are quite flexible on that, but we feel the 30-day period is reasonable. In particular, it should ensure that they get timely advice from us so that they do not make a mistake which ends up costing them a lot of money.

Senator BARNETT—If you have any international comparisons regarding the 30-day period that would be of interest. They indicated they are part of the global marketplace and they do not want to be left behind and come second rather than first.

Mr McDonald—They always say that.

Senator BARNETT—I would say that too if I was them, so you need to have an answer.

Mr McDonald—They take ages to develop new changes and, also, it is very rare that they have not already been implemented somewhere else. What we can do is provide them with assistance drawn from what we know about what is going on elsewhere in the world. I do not know whether our friends here want to add to that.

Senator BARNETT—Let's hear from Mr Windeyer.

Mr Windeyer—I do not think I have a lot to add, other than to reiterate the points Mr McDonald has made that these provisions are consistent with provisions that were in the act up until a couple of years ago and that, from our perspective, the introduction of provisions which encourage early engagement and discussion with relevant agencies to deal with issues is a good thing.

Senator BARNETT—Point taken. If there is a way you think this could be better expressed in the bill or if you think there is a way of mutually agreeing a better way to go, please advise on notice.

Mr Windeyer—Okay.

Senator BARNETT—They have indicated a willingness to work with you, so that is what I would say at this stage.

Mr McDonald—We have always found them a great industry to work with. In particular, the Australian Mobile Telecommunications Association and the Internet Industry Association have been extremely good organisations, and the Communications Alliance too. Maybe they do not quite understand what is expected and we can do some discussions with them.

Senator BARNETT—I have one more quick question on ASIO, Mr Fricker. You may have heard the question I asked earlier about sharing with the minister information that you may gather under schedule 6, items 12 and 17—and perhaps under other places. In what circumstances is that possible and how often would that occur?

Mr Fricker—I was in the room but I did not catch the full discussion. In the broad sense, ASIO's collection activities, or collection using its special powers, are all conducted under warrant by the Attorney-General. The effectiveness of that warrant is reported back to the Attorney-General. So as a routine measure the Attorney-General is aware of the utility, success and intelligence value by way of measuring the performance of those warrants—often because we may be putting up a case for the extension of the warrant or otherwise as part of the ongoing management of the portfolio. I do not think there is anything new being proposed as a result of these amendments. This continues to be business as usual. As I say, it is a window the minister has into the proper conduct of the organisation.

Senator BARNETT—Do you on behalf of ASIO have the same response as Mr McDonald in terms of the Law Council of Australia's concerns regarding schedule 6, items 12 and 17?

Mr Fricker—Yes, I am in agreement. Maybe if I could add to that in relation to the discussions around the national interest, there are a number of thresholds and judgments to be made that this will be information collected by ASIO under its powers with all of the justifications, the purpose and the warrant required to collect that information. Really, what we are talking about here is intelligence gathered incidental to the purpose of that warrant which has significant gravity to make it a matter of national interest. It is not going to be a routine trickle of bits and pieces which are coming out of ASIO investigations where this may be of interest to agency X or this may be of interest to agency Y. These are serious decisions made at the most senior levels of ASIO about what is and what is not the national interest. These are traditional judgments. These are judgments which have always been made by the Director-General of Security. I do not want to leave this committee with the view that we are now going to have a spin-off line of business that with every warrant we have we must produce something for other agencies. It is not that at all. These are serious considerations about what goes to the national interest.

Mr McDonald—And it does not change any of the functions of the agency or any of the agencies.

Senator BARNETT—I have one other question on a different matter for the AFP regarding the New South Wales Police Force and the benefit of amending schedule 3 regarding missing persons. Do you support the view of the New South Wales Police Force?

Mr Whowell—Yes, we do.

Senator BARNETT—So you are happy with that amendment?

Mr Whowell—Yes.

Mr Fricker—Senator, I know you are concerned about the time and I do not want to ask too much of your indulgence, but you did speak before about the imperative to move on this and the timing. Can I just add to the comments of Mr McDonald that the pace of technological change is something which is an imperative to us moving on this. If Australia's national security capability is to be maintained we have to position ourselves such that no agency is disadvantaged because another agency has a technical capability which is unavailable to them under their legal authority to undertake interception or investigative activity. I think the clock is ticking for us to strategically position ourselves, as a national security community, to make sure that this country's interests are best served by the infrastructure that we have across the national security community.

Senator BARNETT—Can I ask the AFP: do you have a similar view to that?

Cmdr Strauss—Yes, we would support that. I guess the the counter-terrorism environment, nationally and internationally, is the perfect example. Without going into specific operations that is the national security interest that would assist us greatly. We support that submission by Mr Fricker.

Senator BARNETT—All right. Thank you for your evidence.

CHAIR—There is something I was hoping you would be able to take on notice for me. The fourth recommendation by the Office of the Australian Information Commissioner goes to clarifying the explanatory memorandum. Can you provide me with a response to that suggestion by them?

Mr McDonald—We will do it.

CHAIR—Can you do it now?

Mr McDonald—We will certainly provide clarification; we will certainly review that—subject to the Attorney-General's approval.

CHAIR—Oh, I see; so you might look at revising the explanatory memorandum when the bill is debated again?

Mr McDonald—I thought that is what they were asking for.

CHAIR—Yes. I am asking for you to respond to us.

Mr McDonald—Yes, and we would be very cooperative in responding to that.

CHAIR—I suppose what I am asking you to do is to provide a response to this committee about whether you believe their view has merit or not. It is the same with the specific comments on the explanatory memorandum—there are four of those—and also a comment about the financial impact at page 2 of the Australian Privacy Foundation's submission. It would be helpful if you could respond to their comments about the explanatory memorandum.

Mr McDonald—There are always ways we can improve the explanatory memorandum, so we will review those comments.

CHAIR—Finally, can I ask you about the issue I raised with Dr Clarke—that is, the matter that is arisen in the Northern Territory in recent days. Is this bill related in any way to that situation? Does it make that situation worse? Should we put those thoughts on hold? No doubt, the journalist shield laws will come to this committee at some stage. Should we wait and raise it then?

Mr McDonald—Yes, I think that is pretty close to my answer that there is quite a bit happening elsewhere on this. Clearly, with the whistleblowing laws and packages that are around, the basic concept of the whistleblowing laws is to provide lawful authority in specific areas, and our criminal code—

CHAIR—Are you talking about the whistleblower who might have rung the journalist?

Mr McDonald—What I am getting at is that there is quite a lot of legislative activity in this area and, in that context, whether it is journalist's privilege or whistleblowing laws more broadly, there is a lot of consultation and work going on. Where something is authorised as lawful, that gives you a lawful authority defence. While I cannot give you a comprehensive issue here and now on this particular issue, I can say that, once all that process is completed, I am sure the position will be quite clear.

CHAIR—I suppose I am flagging to you that, if this committee gets that journalists shield law—I am sure you have been following the media in the Northern Territory. There is a view that the seizure of the journalist's mobile phone records by the police without his knowledge is a backdoor way of not protecting the journalist and his source of information despite the journalist shield laws that may be put in place.

Mr McDonald—As I understand it, the case was to do with disclosure of information so, clearly, it is relevant to it.

CHAIR—We may need to revisit it if we get those laws.

Mr McDonald—I am sure that we will get some clarity in that area as a result of the process.

CHAIR—There are a few bits and pieces to take on notice. We will need those by next Thursday. That seems a bit generous!

Mr McDonald—That is the paradigm we are in!

CHAIR—We are losing all sense of time as we deal with this legislation.

Mr McDonald—That is the great thing about word-processing machines!

CHAIR—Yes, that is true. I thank you all for your attendance this afternoon and for your assistance in getting some clarity around this legislation.

Committee adjourned at 4.14 pm