



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

ENVIRONMENT, COMMUNICATION, INFORMATION
TECHNOLOGY AND THE ARTS LEGISLATION COMMITTEE

Reference: Communications Legislation Amendment Bill (No. 2) 2003

FRIDAY, 5 SEPTEMBER 2003

CANBERRA

BY AUTHORITY OF THE SENATE

INTERNET

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

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

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

WITNESSES

CHEAH, Mr Chris, Chief General Manager of Telecommunications, Department of Communications, Information Technology and the Arts..... 1
..... 29

FORD, Mr Peter Malcolm, Acting Deputy Secretary, Criminal Justice and Security, Attorney-General’s Department..... 1

MADDRELL, Mr Spencer Coghill, Head, Regulatory Compliance Program, Vodafone Pty Ltd 15

McDONNELL, Mr Brian, Policy Analyst, Vodafone Pty Ltd 15

MURPHY, Mr Cameron, President, New South Wales Council for Civil Liberties 23

SMITH, Ms Catherine, Acting Assistant Secretary, Security Law Branch, Attorney-General’s Department 1
..... 29

TEARNE, Ms Anastasia (Anna) Karen Diane, Principal Legal Officer, Attorney-General’s Department 1
..... 29

THOMAS, Mr Brenton, General Manager of Enterprise, Infrastructure Branch, Department of Communications, Information Technology and the Arts..... 1
..... 29

WILLIAMS, Mr Don, Section Head of Telstra Shareholder Policy Branch, Department of Communications, Information Technology and the Arts 1
..... 29

SENATE**ENVIRONMENT, COMMUNICATIONS, INFORMATION TECHNOLOGY
AND THE ARTS LEGISLATION COMMITTEE****Friday, 5 September 2003**

Members: Senator Eggleston (*Chair*), Senator Mackay (*Deputy Chair*), Senators Bartlett, Lundy, Santoro and Tchen

Participating members: Senators Abetz, Bolkus, Boswell, Brown, George Campbell, Carr, Chapman, Conroy, Coonan, Chris Evans, Faulkner, Ferguson, Ferris, Harradine, Harris, Humphries, Knowles, Lees, Lightfoot, McLucas, Mason, McGauran, Murphy, Nettle, Robert Ray, Watson and Wong

Senators in attendance: Senators Cherry, Eggleston and Lundy

Terms of reference for the inquiry:

Communications Legislation Amendment Bill (No. 2) 2003

Committee met at 10.36 a.m.

FORD, Mr Peter Malcolm, Acting Deputy Secretary, Criminal Justice and Security, Attorney-General's Department

SMITH, Ms Catherine, Acting Assistant Secretary, Security Law Branch, Attorney-General's Department

TEARNE, Ms Anastasia (Anna) Karen Diane, Principal Legal Officer, Attorney-General's Department

CHEAH, Mr Chris, Chief General Manager of Telecommunications, Department of Communications, Information Technology and the Arts

THOMAS, Mr Brenton, General Manager of Enterprise, Infrastructure Branch, Department of Communications, Information Technology and the Arts

WILLIAMS, Mr Don, Section Head of Telstra Shareholder Policy Branch, Department of Communications, Information Technology and the Arts

CHAIR—I declare open this public hearing of the Senate Environment, Communications, Information Technology and the Arts Legislation Committee and welcome everybody here today. The committee is examining the Communications Legislation Amendment Bill (No. 2) 2003 which the Senate referred to the committee on 20 August on the recommendation of the Selection of Bills Committee. The committee is due to report its findings to the Senate by next Tuesday, 9 September. Today's hearing will enable us to discuss concerns expressed about the bill in the two submissions we have received.

I now welcome our first witnesses, a panel of representatives from the Department of Communications, Information Technology and the Arts and the Attorney-General's Department, who will open the committee by providing the committee with a summary of the key provisions of the bill before returning at the conclusion of the hearing to respond to any

issues raised during the course of the hearing. I understand that you, Mr Ford, will be unable to rejoin us later because of a pressing commitment, so we will make sure that you are given every opportunity in this first session to make whatever points you wish to.

As I am sure members of the committee and witnesses know, the committee prefers all evidence to be given in public but, should you at any stage wish to give your evidence, part of your evidence, or answers to specific questions in private, you may ask to do so and we will consider your request. I remind all witnesses that the evidence given to the committee is protected by parliamentary privilege. I also remind you that the giving of false or misleading evidence to the committee may constitute a contempt of the Senate. Finally, as you are all public servants, I point out that you will not be expected to answer questions which invite you to express an opinion on matters of policy and that you will be given reasonable opportunity to refer questions to superior officers or to a minister. I would now like to invite you to make an opening statement.

Mr Cheah—We would like to make an opening statement just to give some background on the bill. The Communications Legislation Amendment Bill (No. 2) 2003 implements decisions of the government to enhance the security of Australia's telecommunications services and networks and to improve existing arrangements relating to call data disclosure, interception service and provision of assistance to law enforcement agencies by telecommunications carriers and carrier service providers. The Telecommunications Act 1997 provides the legislative basis for Australia's open and competitive telecommunications industry. The telecommunications industry is attracting significant new investment that increases the potential for national security and law enforcement issues to arise. The telecommunications act requires carriers and carriage service providers to protect the confidentiality of communications and information relating to people using their services subject to certain limited, authorised circumstances where the disclosure or use of protected information is in the public interest.

The Telecommunications Act also requires carriers and carriage service providers to give law enforcement agencies such help as is reasonably necessary in enforcing the criminal laws and laws imposing pecuniary penalties, protecting the public revenue and safeguarding national security. This help can include disclosure of protected information and provision of interception services where appropriately authorised. The government recognises that there may be some circumstances in which the granting of a carrier licence or the provision of a particular telecommunications service may be prejudicial to national security.

The bill amends the Telecommunications Act 1997, which is administered by the Minister for Communications, Information Technology and the Arts; and the Australian Security Intelligence Organisation Act 1979, the ASIO Act, and the Administrative Decisions (Judicial Review Act) 1977, the AD(JR) Act, administered by the Attorney-General. The bill is intended to ensure that national security and law enforcement interests are appropriately considered and addressed in the granting of carrier licences and in the operation of telecommunications services by existing carriers and carrier service providers. The bill contains measures that would give the Attorney-General certain discretionary powers on security grounds to direct the ACA to refuse to grant a carrier licence and to direct a carrier or carriage service provider to cease supplying one or more carriage services.

The legislation has been developed in consultation with the Attorney-General's Department, ASIO, the Australian Communications Authority, the Department of Defence, Treasury, telecommunications carriers—Telstra, Optus, Vodafone, AAPT and Hutchison—and law enforcement agencies. The Department of Communications, Information Technology and the Arts is responsible for, among other things, the development and management of telecommunications policy, legislation and support programs. This includes providing advice to the minister in relation to the Telecommunications Act and associated legislation. The Attorney-General's Department has responsibility for a range of law enforcement and security policy issues. For example, the agency coordinator, a senior official within that department, has a key role in liaising with national security and law enforcement agencies. Provision of interception services is authorised by warrants issued under the Telecommunications (Interception) Act 1979, administered by the Attorney-General.

The bill was drafted primarily in response to the government's consideration of a number of recommendations of the review of the long-term cost-effectiveness of telecommunications interception, also called the Boucher review, and the concerns of law enforcement agencies about the potential ownership of telecommunications companies by entities whose activities may pose a risk to national security. The bill seeks to address heightened concerns about the need to enhance the security of Australia's telecommunications services while preserving the balance provided for in the existing legislative framework between the need to protect an individual's privacy and confidentiality and the public and national interest in having protected information disclosed in limited authorised circumstances.

I turn now to a summary of the main provisions of the act. Amendments to the Telecommunications Act included in the bill will require the ACA to consult with the agency coordinator in the Attorney-General's Department prior to the granting of a carrier licence; allow the Attorney-General, in consultation with the Prime Minister and the minister administering the Telecommunications Act, to direct the ACA to refuse to grant a carrier licence on national security grounds; and allow the Attorney-General, again in consultation with the Prime Minister and the minister administering the Telecommunications Act, to direct a person not to use or supply, or to cease using or supplying, carriage services on national security grounds.

The bill also amends the AD(JR) Act to exclude from judicial review under the AD(JR) Act decisions made by the Attorney-General under the proposed amendments to the Telecommunications Act on National Security grounds. The exclusion of judicial review under the AD(JR) Act is consistent with the existing exclusions under the act for similar decisions based on national security considerations. Judicial review will still be available in the Federal Court under section 39B of the Judiciary Act 1903 and in the High Court under section 75(v) of the Constitution. The bill includes provisions to amend the ASIO Act to introduce an alternative independent appeal mechanism by enabling a carrier licence applicant, a carrier or carriage service provider, to apply to the Administrative Appeals Tribunal for review of an adverse or qualified security assessment that ASIO has provided to the Attorney-General.

The proposed amendments to the ASIO Act will also require the Attorney-General to notify a person of an adverse or qualified security assessment in respect of that person, except where

such notification will be contrary to the interests of national security. This bill also contains several minor amendments to the Telecommunications Act to clarify the existing obligations of carriers and carriage service providers and to introduce new obligations on carriers and carriage service providers to improve the efficiency and effectiveness of current call dated disclosure and interception arrangements under the Telecommunications Act.

The amendments will, first, respond to changes in law enforcement agency management structures and classifications in the definition of ‘senior officer’ in subsection 282(10) of the Telecommunications Act, thereby reducing delays in the issuing of authorising certificates and requiring most categories of senior officer to be authorised or nominated in writing by the Commissioner of Police, the Deputy Commissioner of Police or the CEO of a relevant agency. These proposed changes do not represent either a relaxation of authorisation procedures or of the principle that certificates are to be authorised by persons of appropriate seniority.

Second, the amendments will clarify that when executing a telecommunications interception warrant, carriers and carriage service providers should provide all relevant information associated with that communication—such as the location from which the communication was sent or received and the time, date and duration of the communication, along with the call content—to law enforcement agencies. This information is required by law enforcement agencies at the time that the content of communication is obtained, so that the communication can be interpreted correctly.

Third, the amendments will clarify that the capability to intercept a communication passing over a network facility or carriage service is the fundamental legal obligation to be met by carriers and carriage service providers under part 15 of the Telecommunications Act. Fourth, the amendments will impose a 60-day time frame for the agency coordinator to consider applications by carriers and carriage service providers to be exempted from the obligation that their networks, facilities and carriage services have an interception capability. Under the Telecommunications Act, the agency coordinator may grant exemptions from the obligation to provide interception capability in relation to specified carriers and carriage service providers. At present there is no time frame for applications for exemptions to be considered.

Fifth, the amendments will require carriers and nominated carriage service providers to include in their interception capability plans statements about current and continued compliance with their interception obligations, and will require interception capability plans to be signed by or on behalf of the chief executive officer of the carrier or nominated carriage service provider. This proposed amendment will encourage industry’s engagement with interception capability plans and improved compliance with the interception arrangements as laid out in the plans.

Sixth, the amendments will change the date on which carriers and nominated carriage service providers must lodge their interception capability plans with the agency coordinator and the ACA—from 1 January each year to 1 July each year. This will facilitate timely lodgment of draft interception capability plans by industry, and completion of consultation and amendment processes by the agency coordinator. Seventh, the amendments will change references to the Criminal Justice Commission of Queensland to the Crime and Misconduct Commission of Queensland, which was established in 2002. The package of amendments

contained in the bill will lead to more secure telecommunications networks and services, and improved arrangements for the provision of assistance of law enforcement agencies by telecommunications carriers and carriage service providers.

Mr Ford—As well as appearing in my capacity as Acting Deputy Secretary, Criminal Justice and Security, I am also in my real job head of the Information and Security Law Division. In that capacity I am appointed as agency coordinator, which fills in part of my role here. In 1999 I conducted a wide-ranging policy review of telecommunications interception matters, which was partly in response to commitments made during the passage of amendments to the Telecommunications (Interception) Act 1979 in 1997 and partly in response to globalisation and massive technological changes in the telecommunications industry. In respect of the latter, my principle recommendation, which was accepted by the government, was that there should be provision for a carrier to be required to cease providing services in certain circumstances. The objective was to protect two aspects of national security. First, to deal with the possibility that a carrier might compromise ASIO's ability to execute a warrant issued by the Attorney-General and, second, to ensure that such a carrier could not itself carry out any unlawful interceptions.

To achieve this objective, the bill would amend the Telecommunications Act in two principal ways: firstly, the agency coordinator would be able to examine new applications for carrier licences before they are granted and would endeavour to resolve any security concerns informally if possible or formally if necessary; secondly, if that fails, the Attorney-General, in consultation with the Prime Minister and the Minister for Communications, Information Technology and the Arts, would be able to direct a carrier to cease using or supplying a carriage service. We would expect that the power vested in ministers would be used only as a last resort and its real utility would be as a backup to arrangements with the carrier in question to deal with security issues.

Senator LUNDY—There are three telecommunications bills—Nos 1, 2 and 3—and can you explain for the record what amendment bills Nos 1 and 3 cover, as they are also before the parliament.

Mr Thomas—I am not across the details of communications bills Nos 1 or 3. I am afraid it is outside our particular area. I apologise for that.

Senator LUNDY—I am trying to be helpful because I know there is a lot of confusion out there at the moment about the bills before the parliament.

Mr Cheah—It is fair to say that they are both omnibus bills and both Nos 1 and 3 cover a range of issues. This bill, however, is one with a clear security focus and has all the security related amendments in it. I suppose that is what we have come prepared to discuss today.

Senator LUNDY—That is fine. How extensive are the amendments in this bill to the ASIO Act?

Ms Tearne—The amendments to the ASIO Act are quite minor. They are consequential ones essentially to make sure that there are appropriate review mechanisms for the security assessments that might support a decision by the Attorney in respect of these two direction powers. They are essentially ones that would extend the definition of 'prescribed administrative action' in the act to include action taken under those two direction powers. The

effect of that is to make sure that the review mechanisms that are referred to in the ASIO Act are picked up in respect of these new directions that could remain about security matters.

Senator LUNDY—There are two primary areas that the bill affects: the ability for attorneys-general to play a role, effectively, in vetting the issuing of a carrier licence, and also the issue of intervening in the provision of a telecommunications service by a carrier. Can you tell me what the current power of ASIO is in relation to the interception of warrants. Can you give me some background to the process by which a telecoms interception warrant may be obtained, and what level of proof is required before a phone tap is permitted? I am trying to get a picture of the position now and then test what the bill is proposing to change against that.

Mr Ford—In terms of the licensing aspect, national security does not feature in the considerations that relate to licensing. But in relation to the procedures for getting a warrant, it is set out in the early part of the Telecommunications (Interception) Act. It requires the Director-General to make application to the Attorney-General. The matters that the Attorney has to be satisfied about are set out in the act and they relate to security and foreign intelligence, as defined in the ASIO Act. If the Attorney is satisfied, he issues the warrant for the limited period as prescribed in the act and that is it.

There is a further administrative step that the Director-General has put into that and that is for the warrant to first be brought over to the Attorney-General's Department, to myself or another senior officer, to have a final look at the legalities and so on, and we sign a form certifying that we are happy with that. The Attorney then looks at that as part of his consideration.

Senator LUNDY—The grounds for that are security and foreign intelligence?

Mr Ford—That is right.

Senator LUNDY—Is there anything in this bill that changes the consideration of the grounds upon which a telecommunications interception warrant might be issued?

Mr Ford—No.

Senator LUNDY—So nothing changes there.

Mr Ford—No.

Senator LUNDY—In terms of the words used in the explanatory memorandum and the statement made this morning, there is extensive use of 'national security' as a term. Is that a general encompassing term of security and foreign intelligence or does it mean something new or different?

Mr Ford—My colleagues might wish to say something on this. I think 'national security' is used as a broad term, encompassing security and foreign intelligence. Counter-terrorism is encompassed in the term 'security and foreign intelligence'.

Ms Tearne—'National security' is used as a broad term, but in terms of the amendments contained in the communications bill what they do is link into the existing defined term of 'security' in the ASIO Act, which is quite a defined concept and has a number of heads that are well established.

Senator LUNDY—Thank you for that; that is what I was looking for. You explained the steps in the current process of the issuing of an interception warrant: the Director-General makes application to the Attorney-General and that is considered and you perhaps have a role in that. What level of proof or evidence is required to initiate that process and what is the level of proof generally required for an interception warrant to be issued?

Mr Ford—The act does not spell this out in great detail; it sets out what the Attorney-General must be satisfied of, so the kind of information that the Director-General may bring to the Attorney's attention might vary depending on the circumstances of a particular operation. The starting point is that someone is engaging in activities prejudicial to security, and the application has to set out the grounds. It may set out grounds of surveillance of some kind or some other information that the Director-General has. It changes from case to case.

Senator LUNDY—The point being that has to be articulated as part of the process for the granting of an interception warrant.

Mr Ford—Certainly.

Senator LUNDY—How does that compare with the process required under this bill for the Attorney-General to direct a person, entity or organisation not to use a telecommunication carriage service or, alternatively, for directing a telecommunications service provider not to provide services?

Mr Ford—The common feature is, if we fasten on this security aspect, in both cases the activity has to be in some way prejudicial to security, as defined in the ASIO Act. The Attorney-General would need to have regard to any concerns that were raised by me, as agency coordinator, or by ASIO as to how those concerns related to security, whether they were relevant or whether they were irrelevant, and so on. So, although it is dealing with quite a different situation, there is quite a strong common theme.

Senator LUNDY—Just to get this clear, we know that to get an interception warrant the grounds for that have to be articulated and they have to relate to security and foreign intelligence. Under this proposed bill is it the case that, for the Attorney-General to direct a person or group not to use a service or a carrier not to provide a service, the same process of articulating the reasons has to be prepared and then provided to the Attorney-General in writing for it to be ticked off?

Mr Ford—It does not set out a similar process, but the grounds have to be similar: they have to be prejudicial to security—

Senator LUNDY—How would initiating the request to the Attorney-General be reflected in an accountability trail?

Ms Smith—We envisage it will be a very similar process in that we will have to be able to justify to the Attorney-General, particularly as he will also have to justify it to the Prime Minister and the minister for communications—we would make a submission to the Attorney-General, which would go through all of the steps that were taken prior to making the decision. The amendments will allow consultation with the agency coordinator. We expect that in many cases we will have attempted to resolve issues without going to this point. So we propose from an administrative perspective to develop guidelines and protocols whereby we will have

particular requirements of information that the Attorney-General will need to make his decision. A lot that information may be classified, because it will be given to us by ASIO.

Senator LUNDY—In the same way that material would form the basis for an interception warrant?

Ms Smith—Exactly. He will make a decision based on a recommendation from the agency coordinator.

Senator LUNDY—My understanding is that the Telecommunications (Interception) Act specifies that process in quite a degree of detail. This bill does not specify that process and it implies much greater ambiguity, despite the fact that you might be looking at administrative codes and guidelines. Can you give me a reason why that specificity was not included in this particular bill?

Ms Smith—Essentially the reason was that we found it difficult to structure exactly in legislation the steps that might be taken in every case. We wanted to make it broad enough so there would be flexibility and every case would not be bound to having to go to the Attorney—we could resolve them through administrative arrangements. Certainly, as part of the consultation on this bill, we have talked at length with the Australian Communications Authority about how we will get more information through the Australian Communications Authority from the actual applicants to put things together. It was a decision at a departmental level that, rather than be bound by specific steps that may be inflexible, we should get to work and put together guidelines within the relevant departments afterwards.

Senator LUNDY—The counterargument is that, with something as sensitive as what this bill is proposing and while ambiguity might suit the departmental processes, there are a whole range of other factors. These include the right of the affected parties—be they consumers or carriers or whatever—to have a very clear understanding of what is happening. If it was a departmental decision to leave that specificity out, could it be built into this bill in such a way that reduces the ambiguity of that process but still recognises the way in which that information arrives through ASIO, the Attorney-General's Department or the ACA to take account of that flexibility?

Ms Smith—My honest answer is that it is always possible to look at how we could draft the legislation because that is a matter that we would have to take up.

Ms Tearne—I want to add a few comments about the way the regime works and the flexibility that it incorporates. The proposed bill works at two levels. In the first instance, there is that flexibility to allow security issues to be resolved by negotiation with participants in the telecommunications industry and to allow them to be addressed at that level without resort to the direction making powers. On the issue of the directions, there is a great deal of assurance, I would think, in the process that is set out for making security assessments. For example, the issuing of security assessments by the organisation is quite tightly restricted by the legislation governing that organisation. It cannot make recommendations or express opinions in relation to what is known as 'prescribed administrative action', which these powers tie into, without issuing that in the form of a security assessment. For example, it cannot express opinions that would have that effect without providing it in the form of the security assessment. That security assessment regime is backed up by the review process.

So I suppose we have two levels within the proposed bill. On the one hand we have the flexibility which affords the industry the opportunity to negotiate these issues with the agency coordinator and, through that, with law enforcement and security players. On the other hand, in the event that we have recourse to those powers, there is that regime to ensure that security assessments are only issued in the most extreme circumstances and expressions of opinion cannot be made by the organisation that has the function of looking into security matters without reference to that process.

Senator LUNDY—That takes me to the next point. With that level of flexibility there, my understanding is that the next step in consideration of whether or not the telco is provided with a licence or has their telecommunications service cancelled is to introduce the Prime Minister and the Minister for Communications, Information Technology and the Arts as another layer in making that decision. Can you explain that? At the moment, when you combine that flexible approach—which allows for negotiations and discussions with telecommunications carriers—with an overlaying decision making structure at prime ministerial and portfolio ministerial level, it introduces a huge opportunity for decisions to be made that are capable of factoring in more than just the security issues at hand. I am not saying that would happen, but the structure differs so much from the traditional model of security assessments in a very tight regime—and introduces what could be seen as a political layer of decision making on top—that it undermines the credibility of the purpose of this legislation.

Mr Ford—There was a recognition that this would be a very serious step. The parliament had, a couple of years ago, passed the call-out legislation to do with calling out the armed forces before the Olympics and so on. In the same way as that was a significant step, this would be, perhaps, not of the same order but would be something meriting the same kind of procedure.

Mr Cheah—I will just add to that. It would be a big move. Because it is such a big step, we would want to make sure that the full range of perspectives was brought to bear on the issue. We would certainly want, for example, to make sure we had thought through the implications for the telecommunications industry of taking the step and we would want the opportunity to advise our minister on taking the step. In regard to the idea of having the Prime Minister involved—if there is an issue about balancing national security and telecommunications industry interests, and in terms of the overall public good, it makes sense to have those three ministers involved in taking such a serious additional step. That is the reasoning behind having those other ministers involved.

Senator LUNDY—Are there any other legislated examples of this model of decision making in relation to national security involving a critical infrastructure like telecommunications?

Mr Cheah—There are some other divisions in parts 13 and 14, I think, which already involve the Attorney-General being required to consult with the minister or the minister being required to consult with the Attorney-General before either one of them exercises their powers. Once again, it is the same issue.

Senator LUNDY—Is the Prime Minister involved in any of those?

Mr Cheah—No, I do not think so, but that is because this extra step is an even bigger step.

Mr Ford—The call-out one that I mentioned before, which is part IIIAAA of the Defence Act, does involve the Prime Minister.

Senator LUNDY—So that is the one example you can think of?

Mr Ford—There could be others, but that is the only one I can think of.

Senator LUNDY—I will come back to this point about the step-by-step process in which that might occur. I think I should approach the different scenarios that you have outlined in the bill separately. If we could first turn to the provision of a telecommunications service, my understanding is that the bill would work both ways. These processes would allow a directive to go to a telecommunications carrier or carriage service provider to cease providing a service to an identified customer. Is that correct?

Ms Smith—The draft as it stands certainly appears to do that but the intention was to turn off an actual carriage service to itself, as a carrier or carriage service provider could not provide to itself or any other person or particular service to a group of people out there in the community at large. It was not the intention that it would be targeting an individual service. It was about protecting the telecommunications infrastructure itself and the protection of being able to execute a warrant on a particular carriage service provider.

Senator LUNDY—I am sorry; I do not understand. Can you start again with what the bill was supposed to do and what you are concerned that it does do, particularly this issue of directives to cease the provision of service to either groups or individual customers?

Ms Smith—The intention is to not provide an actual carriage service which would be provided to the population or a group at large. In the case of a carriage service provider, they could provide it for themselves so that it would be like a closed circle.

Senator LUNDY—So what the legislation is aiming for is the ability to shut down either aspects or all of the services that a carrier or carriage service provider provides to their customer base.

Ms Smith—That is right.

Senator LUNDY—So it is aimed at disabling the carriage service provider or carrier.

Ms Smith—It is aimed at disabling a particular service of the carriage service provider.

Senator LUNDY—Like what?

Ms Smith—As an example—and this is not the case, obviously—a particular service might be a mobile service which has been given to a client base where there is a risk that we could not execute a warrant on that carrier or carriage service provider because there is a risk to national security as it may disclose interception capabilities. It may be that the information could be intercepted for their own purposes. It is about undermining the processes that are currently in place to assist law enforcement and national security in executing a warrant.

Senator LUNDY—We will use mobile services as a useful example, but we could use Internet services or we could be talking about—

Ms Smith—It could be any carriage service.

Senator LUNDY—A broadband service?

Ms Smith—Yes.

Senator LUNDY—Okay, so it could be any product, if you like, that a carrier or carriage service provider might create and then sell to the market.

Ms Smith—Yes. It could be any one that falls within the definition of carriage service under the Telecommunications Act.

Senator LUNDY—The idea is that a directive can be issued to cease all services—that whole product being delivered.

Ms Smith—It would be a directive to not provide that particular carriage service. If we are talking about a particular Internet service provider providing a particular Internet service we would say, ‘Please don’t provide that particular service because there is a risk to security.’

Senator LUNDY—Okay. With regard to definitions, does this apply to Internet service providers as well as carriage service providers and carriers?

Ms Smith—Yes. There is no different definition under the legislation for Internet service providers; they fall within the definition of a carriage service provider.

Senator LUNDY—So it could be a retail ISP service?

Ms Smith—If they are actually providing a service. But a service is distinct to the provision of us being able to access the Internet, not putting up a webpage or that sort of thing—it is the actual service.

Senator LUNDY—Under the Telecommunications Act.

Ms Smith—Yes.

Senator LUNDY—I am getting there. The next scenario in that context is: if the provision of that service created either a security hole or a vulnerability that in the view of the security agencies represented a threat to national security, would that be the basis of the justification for a directive to the carrier or carriage service provider to cease delivering that product in the Australian market?

Ms Smith—Yes, it may be. That is right. But if there was a concern that there might be particular personnel in a particular carriage service provider that were at risk, it may be that we will attempt prior to that to say, ‘We want the warrants to be just looked at by these particular people,’ and that will get around. So we will attempt administrative things before that.

Senator LUNDY—So you will chat to them first and say you have got a problem?

Ms Smith—Yes, that is right.

Senator LUNDY—And you give them an opportunity to fix it?

Ms Smith—That is right.

Senator LUNDY—In the context of that power that you are trying to create, how could that possibly leak into a power that would enable a directive to go to a carrier or carriage service provider to cease the provision of a service on the basis not of the security merits of the product per se but of the potential national security breach by the customer? Does this bill

have any scope to go into those areas, or to create a directive on the basis of that sort of justification?

Ms Smith—As I said earlier, the intention is what we have just talked about. In the legislation as it is drafted, there is scope because it talks about providing it to a person, to actually request that they cease to provide it to a particular service that a person is actually using. However, as I said, that is not the intention, because this is about—and all the policy behind it, which came initially out of Peter's review and that sort of thing, is about—the risk to the telecommunications industry in executing warrants. Normally that person is not posing that risk to national security in the way envisaged by this legislation.

Senator LUNDY—My understanding, then, is that, if the security agencies identified someone who was perhaps attacking or exploiting a vulnerability in the telecommunications network via an identifiable product by a particular carrier or carriage service provider, the only power under this bill to put that person out of business or to prevent them from doing that would be to shut down the whole product as opposed to targeting that individual.

Ms Smith—No, I think that the way the legislation is drafted you could target the individual, but I think—

Senator LUNDY—Under this legislation, or would you be using different powers under different legislation?

Ms Smith—I was just going to say that some of that moves into the critical infrastructure section work and also within the Criminal Code areas.

Senator LUNDY—I would assume that it would move into the Telecommunications (Interception) Act anyway, and other powers that you have to intervene, where you can identify illegal activity or activity that poses a national security threat—it would not actually come through this bill.

Ms Smith—The Telecommunications (Interception) Act is clearly about gathering intelligence, so it is kind of at the other end of the spectrum. You do not want to close someone down because you are wanting to gather the intelligence.

Senator LUNDY—So that is not a good example.

Ms Smith—Putting that aside, there is other legislation—there are offences under the Criminal Code of doing particular things against telecommunications. Peter knows a lot more about the critical infrastructure, but there are dealings at another level as well.

Mr Ford—The critical infrastructure one perhaps is not fruitful to explore unless you wish to, Senator, because it rests so much on voluntary cooperation.

Senator LUNDY—I do want to go there. It concerns me that what we are really talking about are the security merits of different products operating in the telecommunications market here. This bill creates an environment in which the scenario is that someone—presumably ASIO or the defence and security agencies—makes an assessment that the security is not up to scratch and then initiates a process to deal with that, by negotiation or whatever, potentially leading to a directive to shut down a product; and yet there are no standards. There are no standards on critical infrastructure protection or security in relation to the security merits of telecommunications products and services in Australia. If there are, they are obviously not up

to the standard the security agencies would like to see, because then you would have a regulatory pathway to enforcing the security you are looking for, would you not?

Mr Ford—The objectives that I outlined before encompass both deliberate interference with ASIO's execution of a lawful warrant and accidental interference, and it is in that latter category that I recognise that the question of standards is relevant. The only thing I can say on that at this point is that we are addressing the critical infrastructure issue in a different way, not through legislation but through—

Senator LUNDY—Through cooperation and the goodwill of the industry.

Mr Ford—That is right.

Senator LUNDY—Excuse the pun, but there seems to be a disconnect between what you are trying to achieve here using extensive and fairly ambiguous powers to create a mechanism to stop something happening and the fact that in all the other areas where those standards could potentially be achieved the government has chosen a very light-touch approach—in fact there is not even an industry code at this stage. On one hand we see heavy-handed ambiguous intervention involving everyone up to the Prime Minister, but on the other hand we see what could be argued is a very laissez-faire attitude towards critical infrastructure protection and the security standards operating in our telecommunications environment. That inconsistency has become apparent.

Mr Cheah—I am not sure I would characterise it in the way you have. We have several strategies for cooperating with the carriers, and most of them—almost the entire industry—are very cooperative. But you do have to at least be prepared for the possibility of exceptions, particularly in the current environment. The other point I want to make is that we have a multilayered approach to things. For example, carriers have to have an interception capability plan. That is one of the ways in which the agency coordinator gets to regularly communicate with the carriers about their interception needs and what have you. As an example of one of the potential gaps, what do you do in a situation where the carrier or carrier service has a legal obligation to have an interception capability but does not address it and keeps on not addressing it? What do you do?

Senator LUNDY—That is not what I am arguing about; I think that is a separate issue. If there are obligations to have those capabilities and to be able to demonstrate that, I recognise that a number of the amendments put time frames around that and create a great deal more certainty for the carriers about what their obligations are. My points go beyond that to the ability of telecommunications carriers to understand what is involved when there are no standards out there. It becomes very ambiguous when there are a lot of companies investing in networks and a lot of customers paying a lot of money to access those services. This potentially creates uncertainty in relation to that—notwithstanding the admirable efforts to tighten up national security, of which there are some elements here. At this stage I am trying to get a better understanding of the broader—

CHAIR—Senator Lundy, we will have a session at the end to do with general issues. There are still two lots of submitters to give presentations and we are now 25 minutes over time, so we might bring these witnesses back at the end.

Senator LUNDY—Perhaps we can wrap this up. Is it possible, under the bill as currently drafted, for a directive to be issued to disconnect a phone service of an identifiable group or individual customer on the grounds of national security?

Ms Smith—As it is drafted, it certainly appears that that is the case for an individual service. As far as a group goes, it would have to be an individual application or—

Senator LUNDY—What about an individual customer?

Ms Smith—Yes, as currently drafted.

Senator LUNDY—Was that intentional?

Ms Smith—No. The intention was to address it as a carriage service but, because of the way an individual is defined, an individual could be a company, an Internet service provider or an individual. That is why it is addressing it as an individual.

CHAIR—Thank you very much for appearing.

[11.26 a.m.]

MADDRELL, Mr Spencer Coghill, Head, Regulatory Compliance Program, Vodafone Pty Ltd

McDONNELL, Mr Brian, Policy Analyst, Vodafone Pty Ltd

CHAIR—Welcome. The committee has your submission before it, which it has already published. Do you wish to make any alterations or additions to your written submission at this stage?

Mr McDonnell—No.

CHAIR—Senator Cherry will take part in this session by phone. The committee prefers all evidence to be given in public but, should you at any stage wish to give your evidence, part of your evidence or answers to specific questions in private, you may ask to do so and we will consider your request. I remind the witnesses that evidence given to the committee is protected by parliamentary privilege and that the giving of false or misleading evidence to the committee may constitute a contempt of the Senate. Would you like to make an opening statement?

Mr Maddrell—Yes, please. Vodafone welcomes the opportunity to appear before the committee today. As you may be aware, Vodafone is the world's largest mobile phone company. Vodafone has operations in 28 countries across the world, working within a wide range of economies, geographies, cultures and regulatory regimes. To set in context the size of the Vodafone group, 25 per cent of the world's mobile phone users are connected to Vodafone.

Vodafone is a wireless communications specialist offering innovative wireless solutions to corporate, government and consumer users of both voice and data connectivity. Vodafone in Australia is the third largest mobile provider. We currently have a customer base of 2.6 million customers. Vodafone has been operating in Australia since 1992. From this time, Vodafone has been a major investor in the Australian telecommunications industry, having invested billions of dollars in the roll-out and expansion of state-of-the-art GSM and GPRS networks and associated products and services to work over the networks. Furthermore, Vodafone, as the third largest player in the mobiles market, has played a significant role in bringing competition to the marketplace, which undoubtedly has facilitated greater consumer offerings in that marketplace.

Vodafone acknowledges that telecommunications is an important national sector essential to the proper functioning of the government, its people and the economy. Set in this context, Vodafone acknowledges that telecommunications will inevitably be relevant to consideration of national security issues, particularly given the current domestic and global security environment. We are committed to our statutory obligations to assist law enforcement and national security agencies to achieve such outcomes, as evidenced by the level and quality of service we currently extend to such agencies in the lawful disclosure of information and the provision of unlawful interception.

Accordingly, Vodafone supports the object of the bill: seeking to ensure that Australians are protected from threats to national security through the misuse of telecommunications facilities and services. Indeed, we acknowledge that it is necessary and appropriate for the government to have adequate powers in seeking to protect Australia's national security. While we

acknowledge such objects and their importance, we believe that any government powers that have the potential to interfere with the legitimate business practice of telecommunications providers, including Vodafone, must be no wider than is strictly necessary to protect against the risk to national security, and that there should be appropriate checks and balances in place regarding their exercise. The bill as currently drafted will confer very wide discretionary powers that could conceivably result in such interference. Therefore, we believe that an amendment could be made to the bill that would maintain the objects and intention of the bill while also balancing the legitimate business interests of private firms that may be impacted by the exercise of such powers.

In particular, we are concerned that new subsection 581(3) added by the bill will confer a very broad power on the government to direct carriers and carriage service providers not to use or supply, or to cease using or supplying at all or to particular persons, a carriage service or all carriage services where such use or supply is considered to be prejudicial to national security. It must be noted that Vodafone is already subject to legislative obligations under section 313 of the Telecommunications Act to give reasonable necessary assistance to officers of the Commonwealth, states and territories in enforcing the criminal law, protecting public revenue and safeguarding national security. We believe that under the above power Vodafone would be required to extend such assistance as required by the circumstances. Thus, in the context of an extreme threat to national security, we would provide such assistance as was reasonably necessary in the circumstances.

The passage of the current bill suggests that the government believes that there is a need to give the Attorney-General additional explicit powers to direct carriers and carriage service providers to cease supplying carriage services in extreme cases of prejudice to national security. Accordingly, we believe amendment and improvement to the bill should be made and that such amendment and improvement should be guided by the principle of proportionality. Thus, given the potential impact of the bill on the telecommunications provider's business practice, the power granted and exercised under the bill should be proportional to the threat posed to national security by the misuse of telecommunications facilities and services. Applying this principle, we submit that the power should be amended so that it is limited to directing a carrier or carriage service provider to cease supplying a carriage service to a particular person or persons with access to the carriage service where use of the carriage service by that person or persons poses a threat to national security. Currently, the drafting is much wider than this, extending to the ability to give the carrier or carriage service provider a direction that it cease using or supplying carriage services generally.

Amendment should also be made to include an express legislative requirement that the power be exercised only where there are demonstrated grounds that this is necessary to protect national security and only where the risk to national security cannot be managed effectively through other mechanisms. The current drafting of the power omits such a requirement, which effectively means that the power could be used in alternative circumstances. Such an express legislative requirement would provide greater certainty to carriers and carriage service providers that such powers could only be relied on in national security circumstances.

Vodafone submits that a further required amendment is for the power to provide statutory immunity with respect to acts done in good faith and in compliance with a direction under the power. Importantly, sections 313 and 315—which, respectively, require carriers and carriage service providers to give reasonably necessary assistance and provide power for senior police officers to request that a carriage service be suspended—carry such an immunity. In the absence of such a power, carriers and carriage service providers could potentially be exposed to very significant claims with respect to damages for ceasing to supply telecommunications services to their customers. A statutory immunity similar to that provided under sections 313 and 315 would give carriers and carriage service providers greater certainty in their business practice as to where they stood in relation to the exercise of such a power.

We believe that should the above be rejected the bill could be amended to provide more meaningful administrative review rights. Should the power be amended along the lines we have suggested, we contend that the requirement for the inclusion of more meaningful judicial review rights are less important as the exercise of the power would be constrained by the drafting. However, in the absence of such constraint, the inclusion of more meaningful review rights becomes imperative as the wider discretion creates uncertainty for carriers and carriage service providers as to how the power may be exercised. Accordingly, review rights may be the only mechanism through which carriers and carriage service providers may be able to challenge the legitimacy of the operation of the power.

We submit that provision should also be made in the bill for compensation of carriers and carriage service providers for any costs they incur and loss and damage they suffer as a result of directions under this section. Such compensation would again be consistent with similar provisions currently operating under the Telecommunications Act and should be provided to again facilitate greater certainty to carriers and carriage service providers. The issue of certainty is an important one in the telecommunications industry, which is highly capital intensive. Providers of telecommunications need such certainty in order to make informed decisions on whether to invest in expansion or development of networks and services. In the absence of such certainty, the decisions to invest may be prejudiced. We would be happy to answer any questions the committee may have regarding the issues we have raised.

CHAIR—Thank you very much. We might go to Senator Cherry, who, as I said, is with us via teleconference.

Senator CHERRY—My first question is a fairly obvious one. Why do you think that other telephone carriers have not actually put in submissions of concern about this bill?

Mr Maddrell—We cannot really speak on behalf of the other carriers, but we have decided as a corporate citizen to respond ourselves.

Senator CHERRY—The New South Wales Council for Civil Liberties, which is appearing this afternoon, has suggested that the flow-on effects of this bill have not really been thought through in terms of the processes to be used to minimise legal liability for carriers and so forth. I know you touched on that in your submission but did you think there is a need for a comprehensive rewrite on that side of the bill?

Mr McDonnell—In terms of providing immunity from liability—is that the question?

Senator CHERRY—It is partly about liability and partly about the processes to be followed.

Mr McDonnell—Certainly in respect of liability Vodafone believes that greater immunity provisions are required and indeed necessary under the bill. In terms of the processes, greater clarity and certainty is the basis upon which Vodafone is making its commonsense submission today. So there needs to be greater clarity and certainty on when the power would be relied upon and greater clarity and certainty in terms of the consequences of those powers as well.

Senator CHERRY—Are you concerned about the possible expansion of the scope for telephone interceptions under this bill?

Mr McDonnell—I think that the scope for telephone interceptions is clearly provided for under the interception act and I do not see why there would be reliance on this provision in absence of those provisions under the interception act.

Senator CHERRY—I think at this stage the other stuff is dealt with adequately in your submission. I might come back to questions later.

CHAIR—I have a couple of questions also in terms of your proposed amendments. You speak about the power under section 581(3) only being exercised where there are demonstrated grounds that this is necessary to protect national security and only where the risk to national security cannot be managed effectively through other mechanisms. So you seem to be saying that you want more specificity there. Do you want to expand upon that a little?

Mr McDonnell—It is just simply on the basis, as we have said already, of providing carriers and carriage service providers with greater certainty as to when the power would be relied upon and exercised. That would set a clear delineator. As it is presently drafted it is possible, based on the very wide wording of the power currently, that it could be used for alternative purposes. I do note that the power has been addressed in the second reading speech—that it is relevant to national security issues. However, the mere mention of that in the second reading speech or in the parliamentary process is not sufficient—it needs to be legislatively enshrined.

CHAIR—You also say the Attorney-General must have reasonable grounds to believe rather than just consider that there is a relevant prejudice to national security and that would fit under the same heading.

Mr McDonnell—Yes. As it is currently drafted, we believe that there would be a subjective element to the determination of the Attorney-General in exercising the power. We believe that a necessary addition would be to provide that there be reasonable grounds to consider. At present it merely says that the Attorney-General considers that this would be prejudicial to national security.

CHAIR—The last one is the question of judicial review. We have heard from DOCITA that judicial review will still be possible, but you say that you want meaningful judicial review. I know that because of national security issues there are difficulties in getting a review under the Administrative Decisions (Judicial Review) Act, but judicial review is still available in the Federal Court under section 39B of the Judiciary Act and in the High Court under

section 75(v) of the Constitution. Do you want to expand on your views about judicial review? It would seem that there is a process there.

Mr McDonnell—The comment about meaningful review is linked back to the point which we made before, that the clause as currently drafted states that the Attorney-General considers that the provision of the carrier services is prejudicial to national security. We believe that it would be difficult to appeal a decision or direction, on the basis that as currently drafted that would be a subjective determination by the Attorney-General, which is difficult to challenge at law. However, if we amend it with the provision of words such as ‘reasonably considers that it is necessary’, we believe that would provide greater basis and greater certainty to us in exercising our review rights at law.

Senator LUNDY—Going to this issue of the possibility of subjective elements being introduced into the decision making process, you mentioned alternative reasons—I think they were your words. What is your fear? What is the worst-case scenario in terms of how that ambiguity about how the power can be used, from Vodafone’s perspective?

Mr McDonnell—I do not think we have really thought that far in terms of what our fear would be. As indicated already, our comments today are informed on the basis of affording us greater certainty, because as currently drafted it is very wide and very discretionary.

Senator LUNDY—So you want to remove subjectivity and have very clear definitions on the basis of justification of any decision in relation to directives under this legislation?

Mr McDonnell—Yes, essentially.

Senator LUNDY—In hearing evidence from the department, who appeared before you, we explored the issue of the targeted impact of the directive. The department expressed the view that the aim was to really initiate the shutdown of a product offered by a carrier or carriage service provider, which would obviously have a broad impact. Based on your submission, you are gravely concerned about that. In fact, you argue that a narrower directive to shut down individual customer services is a better way to manage the national security issues, an approach which we now know from the department was not the original intent of the bill. Can you first comment on Vodafone’s response to the directives being associated with a whole product that you offer? We were using mobile phones as an example, which is probably pertinent, given you are Vodafone. Respond to that and then I will come back to the other issue about individual services.

Mr Maddrell—A directive to shut the entire network for a period of time would be one which Vodafone would never recover from. I find it difficult to identify circumstances in which that would be necessary, hence the drive towards greater specificity.

Senator LUNDY—If that remains a feature of the bill, do you think the bill is workable or that it should pass?

Mr McDonnell—The power to make directives to facilitate the provision of greater certainty to the government and national security agents in the context of national security issues is certainly a valid power for the government to have, and Vodafone can certainly foresee the need for that power. However, as we have stated, we believe that the terms in which it is currently drafted are too wide and would inevitably create difficulties in the future as to certainty about where it would be exercised.

Senator LUNDY—To make a finer point of it, how many products does Vodafone offer as a telecommunications carriage service provider?

Mr McDonnell—I do not know the exact number. We have a range of products and services.

Senator LUNDY—But they all operate through pretty much the same infrastructure?

Mr Maddrell—A lot of it is over similar carriage and similar infrastructure—different parts of it, perhaps.

Senator LUNDY—So a directive being issued for you to shut down a whole product or service that you provide is one you think Vodafone would be unable to recover from?

Mr McDonnell—It depends on the scope of that direction. It could be to Vodafone as a whole—all carriage services that Vodafone supply—or the identified person under the direction could be a customer that Vodafone had an agreement with to provide wholesale services to. So the impact it would have on us or on our services really depends on the scope of the direction.

Senator LUNDY—I will come to that. The other scenario is that you receive a direction to shut down a particular individual that you are providing a service to. My understanding is that that is not a scenario the bill is designed to enable but in its current drafted form it would. If you received such a direction, does the bill describe your obligations to advise that customer of your receipt of the direction or give you lines to convey to someone who is having their phone service shut down because they present a national security risk? What in the bill provides direction and advice to you, the carrier, as the party that is being asked to effectively breach a commercial contract with a paying customer?

Mr McDonnell—At present there is nothing, as far as I can see.

Mr Maddrell—That is why we would like the statutory immunity as well.

Senator LUNDY—Would it be useful for Vodafone if the bill did articulate your rights, roles and responsibilities in that scenario?

Mr McDonnell—As I have said, we advocate greater certainty and clarity in the bill.

Senator LUNDY—So that could be an element of it?

Mr McDonnell—That would certainly be an element of it.

Senator LUNDY—As a service carrier in Australia, what is your involvement in the continual assessment and maintenance of the critical infrastructure protection and security standards of your network? I do not want to put you on the spot, but can you comment on those things in the context of this bill, which is asking you to tick a whole lot of boxes to do with things that you do not know about?

Mr McDonnell—In terms of critical infrastructure, we have processes in place to ensure the security—physical and otherwise—of our facilities. They are governed by relevant Australian laws and Vodafone Group requirements. I also note that Vodafone is involved in a Commonwealth government initiative to form guidelines and processes for critical infrastructure protection and security.

Senator LUNDY—The bill provides for an obligation—and I understand that you already have an obligation—to facilitate interception. Can Vodafone comment on the impact of the bill on those arrangements and how they strengthen them, and the likely impact on Vodafone’s ability to ensure that you have a service that is capable of being intercepted under the provisions of the Telecommunications (Interception) Act?

Mr McDonnell—I think that would be a matter more for discussion by the department and Attorney-General’s in terms of the policy behind the bill. Obviously, if we have no carriage services we cannot intercept. That would be one conclusion from that.

Senator LUNDY—I think that is part of the point being made, which is that a number of the provisions of the bill do relate to defining a clearer path for the government to be assured that you have a network and provide services that can be intercepted and which change deadlines and dates about your reporting obligations under those. Do you have any problems with those elements of the bill?

Mr McDonnell—No; we support those elements of the bill. As we noted in our opening statement, we already engage the agency coordinator quite frequently in terms of our role in providing lawful interception over our network, and we support those requirements.

Senator LUNDY—We also heard from the department that a possible scenario is that security agencies found that a vulnerability in your services was being exploited; that they would attempt to work with you to resolve those issues. Does that fit within Vodafone’s understanding of how the bill would operate; and, indeed, how does it relate to current practice?

Mr McDonnell—In terms of how the bill would operate, we really cannot speculate about that. As we said, there is no real guidance provided under the bill about that.

Senator LUNDY—There is nothing in the bill which says that national security agencies have an obligation to at least discuss with you or consult with you prior to any—

Mr McDonnell—That already exists under relevant legislation. As to the circumstances today, as I have noted, we engage regularly with the agency coordinator and agencies to facilitate assistance.

CHAIR—Senator Lundy, at 12 noon we have the New South Wales Council of Civil Liberties.

Senator LUNDY—We should go back to Senator Cherry now and see whether he has any more questions.

CHAIR—I wonder whether we could go to him.

Senator LUNDY—Certainly.

CHAIR—Then, if necessary, we can get Vodafone back. Senator Cherry, do you have any more questions?

Senator CHERRY—I have one question about judicial review. The *Bills Digest* on this bill suggests that there is a real problem with judicial review. A judicial review is only allowed on security clearance grounds, but the person may not know that they have in fact had an adverse security assessment. Vodafone is arguing that the judicial review provisions are

largely fixed if the underlying legislation is tightened up. Doesn't that still fail to get around that issue?

Mr McDonnell—Our statement is that the requirement for more meaningful judicial review rights is less relevant if the power and the extent to which the power could be relied upon and exercised is clearly defined, whereas at the moment it is quite broadly drafted and quite discretionary in nature. The flip side of that is that you would require more meaningful judicial review rights so as to challenge the boundaries to which that power might be exercised or relied upon.

Senator CHERRY—That is all I have at this stage, Chair. Thank you.

Senator LUNDY—You have covered the issue about compensation. As far as the question of statutory immunity and not having any liability goes, are you aware of any other circumstances or is Vodafone aware of any other scenarios—either here or in another jurisdiction—in which statutory immunity applies?

Mr McDonnell—In the Telecommunications Act at present, under sections 313 and 315—which require Vodafone and other carriage service providers to give reasonably necessary assistance to law enforcement, national security and so on—statutory immunity is given to officers, agents, police and so on who act in good faith upon any request for assistance under those relevant sections. We feel that this analogous to that; it is merely an extension of it.

Senator LUNDY—Finally, I want to ask about the scenario in which Vodafone could find itself at the receiving end of a directive to shut down an individual's service provision. I guess the scenario would be that you have been advised that a particular service being provided to a particular individual is creating a security risk. If you were to shut down that particular service—and I am trying to get to the nuts and bolts of this—is that just a question of you terminating that service provision? Can you just do that—that is, make a phone call, make that happen—and that person can no longer use their mobile phone? Is that possible?

Mr McDonnell—It is technically possible, but in terms of executing our duties under the act we have to be certain that we are acting within the law. We have processes and procedures to engage in that assessment. We think it would be beneficial to provide greater certainty and clarity of the amendment to section 581(3) so that we could be certain that we were acting lawfully as well.

Senator LUNDY—In that scenario you would want to be given a period of time in which you could make those assessments as a company?

Mr McDonnell—We are currently under relevant legislation, and I would imagine that would extend to this power. We want that certainty as well.

Senator LUNDY—So that is another area of uncertainty. Thank you.

CHAIR—Thank you very much. If you have any additional material you want to submit, please to do so within the next few days because our reporting date is next week.

Mr McDonnell—Thank you.

[11.59 a.m.]

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

CHAIR—I now welcome by teleconference Mr Cameron Murphy, President of the New South Wales Council for Civil Liberties. This is Senator Eggleston speaking, and I am the committee chairman, and I am accompanied by Senator Lundy from the ACT. I understand you are speaking to us during a break in court proceedings in Penrith, so I am grateful to you for making yourself available at such short notice. The committee have your submission before us, which we have already published. Do you want to make any alterations, corrections or additions to that submission?

Mr Murphy—No, I do not at this stage. I want to apologise for a few typographical errors given the short time that there was to make a submission.

CHAIR—We are operating within a very tight time frame. The committee points out to you that we prefer all evidence to be given in public but should you at any stage wish to give your evidence, part of your evidence or answers to specific questions in private you may ask to do so and we will consider your request. You are also reminded that the evidence given to the committee is protected by parliamentary privilege and the giving of false or misleading evidence to the committee may constitute a contempt of the Senate. Would you like to make an opening statement?

Mr Murphy—I would like to make a short statement. It is our view that this bill has been drafted without giving proper consideration to the practical implications of its implementation. It seems to show a lack of understanding in particular about the operation of the Internet, for example. It is our view that it is inadequate to have in place a procedure where someone's communications service can be terminated without giving them the practical option of quick review. We have seen in other areas where this type of legislation operates that even the simplest of mistakes can occur where the wrong person might have their service terminated. It requires a process of review so that, when an error is made or if there is not sufficient information to show that someone is a national security risk or that national security interests are at risk, action can be taken to restore the communications service that is terminated.

It is also our view that there has not been sufficient consideration given to the way in which telecommunications carriers are supposed to implement this. I do not think that there has been enough time or a clear time frame provided to them. There are still questions over the liability: if they should do their best to attempt to carry out an instruction to terminate a service, what are the effects going to be and who will be liable if they make a mistake or if, for example, they terminate the service of many people when they are required only to prevent access by one person? I will leave it at that because of the short time frame today and I would be happy to answer any questions the committee might have.

Senator LUNDY—Going to the issue of judicial review, firstly, we heard from the department earlier, who described a secondary judicial review process, which did provide some avenues under the Federal Court under section 39B of the Judiciary Act and under the High Court under section 75(v) of the Constitution. Can you comment on how that relates to what you are talking about with the inadequacies of judicial review in the current bill and

whether those secondary pathways, if you like, are meaningful if anyone had issue or complaint about how decisions were made under the bill as it is currently drafted?

Mr Murphy—The problem as we see it under the bill as it is currently drafted is that it is all well and good to say there are these avenues through the Federal Court and High Court that allow for judicial review but what you are talking about practically, when this is put in place, is that the Attorney will make a decision requiring a carrier to terminate a telecommunications, Internet or email service. The ordinary punter on the street has virtually no capacity to take a matter to the Federal Court or the High Court, at significant expense, particularly given that they are unlikely to know the reason why their service has been terminated. It is well and good to say that that is an option that is available, but it is an option that is so limited that almost no-one using these services in Australia at the moment would be able to afford to take that action to have their service restored. So you cannot characterise this as a way of review in practical terms.

Senator LUNDY—The second point in your submission talks about the bill significantly increasing the information that will be available under interception warrants in that it requires more than just the content of the communication to be provided. Are you able to explain to the committee your concerns in that area, particularly in the context of what you have identified as a general increase in surveillance in Australia? I presume you are talking about the Telecommunications (Interception) Act 1979 there.

Mr Murphy—Yes. We have a serious problem in Australia at the moment. Because of efficiency particularly, we have had a massive explosion over the past decade, and in particular over the last three to five years, of the number of telecommunications interception warrants issued in Australia. There are more warrants being issued in Australia, for example, than there are in the entire United States. There is a propensity, when investigating a problem, for law enforcement agencies to apply for a warrant, intercept telecommunications and then progress the investigation from there. We also see a relatively low rate of prosecution as a consequence of those interceptions. So what we are finding is that more and more people are being subjected to surveillance, and many of those people are never convicted of an offence arising from that.

The bill provides another power that would effectively increase the scope of interception warrants so that they would include all relevant information about any communication. A wide terminology is being used. The explanation provided in the explanatory memorandum, as I understand, suggests that this is so that technical data relating to the communication can also be provided. The way it is defined at the moment means that all relevant information has to be provided. If it is simply an issue about technical data, it should be limited, in our view, to technical data. This is a convenient way for an expansion to take place where other information relating to the communication—perhaps records, billing arrangements and so forth—could also be obtained once this warrant is obtained.

Senator LUNDY—On the issue of an expansion of the scope of the interception warrants, you cite section 313 as being the vehicle for that to occur. Is that an area that should be covered by the Telecommunications (Interception) Act 1979 and the definitions under that act? What is your view about using this bill to expand those definitions of what can be intercepted?

Mr Murphy—The real concern that we have is that national security, which is a fairly ill-defined and wide ranging term, will become another reason to have an interception warrant made available to intelligence or law enforcement authorities. That could become quite a convenient way in which they could obtain a warrant which they would not get under existing legislation. If they could not, for example, meet requirements for the issuing of a warrant then a claim could be made that there is a national security interest in the issuing of such a warrant. That could become a back door, if you like, where agencies could obtain a warrant where they would not otherwise get one. They could use national security as a reason to further an existing investigation.

Someone may be under suspicion of importation of drugs, for example, and there may not be enough information, once presented to a court, to obtain a telecommunications interception warrant. So all they do is go through another avenue to the Attorney-General and suggest that the people who are suspects are linked to terrorist or other groups and they require an interception warrant on those grounds. Information obtained there is perhaps used to either further the investigation in the other area or to prosecute the people.

Senator LUNDY—If the definition of what constituted national security were tightened up sufficiently in this bill, would that reassure you as a means of preventing the exploitation of national security as a back door for the investigation of criminal matters or other matters?

Mr Murphy—I think that needs to be done. It is quite unclear. At the moment I am concerned that things like industrial action, political protest, dissent and organisations that do not share the view of government could all fall within this definition of national security. The committee should seriously look at making specific exclusions for particular groups, as it has done in other legislation. The defence amendment aid to civilian authorities act, for example, excludes the engagement of the Defence Force in cases of political protest, industrial action, consumer boycotts and so on—along with other pieces of legislation—and that is one way to preclude its operation. We are also concerned that there is a general increase in the powers that are being provided. There should be a clear definition of national security, and it should be limited in the way that it is defined, otherwise virtually anything could fall within a broad definition allowing these powers to come into play.

Senator LUNDY—You mentioned a series of exclusions that relate to another piece of legislation. Was that the defence call-out legislation?

Mr Murphy—That is what it is. It is the Defence Legislation Amendment (Aid to Civilian Authorities) Act 2000. It has certain exclusions in it for trade union protests and so on, which mean they cannot be called out for such action. It would be prudent for the parliament to accept a wide definition or even a limited definition of national security to at least exclude acts of political dissent and discourse, boycotts, consumer activity, trade union activity and general protest. I do not think the intention of the bill was for it to be used in a situation where the Attorney believes that an environmental protest, for example, is a national security risk.

Senator LUNDY—I want to ask the same question in the context of telecommunications services, because that is the auspice of this bill. A scenario that comes to mind is the use of the Internet—say, an individual's use of a server to provide Internet content and perhaps to initiate an online campaign that might form part of or represent a protest. Is that the analogy you are trying to draw between this bill and the defence call-out legislation?

Mr Murphy—Absolutely. To give you an example: there are a number of web sites out there that members of government of all political parties dislike—the Islamic youth group site, in particular, has been mentioned in the media and web sites like the S11 protest site and so on. While people might disagree with the messages they are sending, and disagree with the sort of political discourse they are engaging in, in a democracy we have to tolerate different views and different ideas.

This legislation could be used to effectively censor organisations like those, where a decision is made that the service must be terminated on the grounds of national security and the plug is pulled on the email, Internet or even telecommunications—mobile phones, landlines—of people who are in these groups. The real danger is that it can be used to censor not only political groups but other groups, as long as they fall within a broad definition of national security. That is something that is not a public and open process; that is something that the Attorney-General is going to be deciding in private, based on limited advice from agencies which might have a vested interest in providing a particular type of advice.

Senator LUNDY—In your reading or understanding of the bill so far—and I acknowledge you have had limited time to investigate the bill and prepare your submission—would the directive extend beyond carriage service providers to content providers, which could, depending on the definitions, be seen as Internet service providers by virtue of the presence of a server in a private premises, for example?

Mr Murphy—In our view it seems to. We have not had enough time to consider it properly, but it could operate as such if you imagine it like a domino effect, where the Attorney gives an order to the telecommunications carrier to terminate the service of a particular person and then that is carried down through the process of your Internet service providers and so on until the action is carried out. On that note, there are a lot of practical problems in doing this. The bill seems to show a lack of understanding about the Internet, because if a particular service to a particular organisation—they might have a web site, for example, with some pages that are supposed to be a national security risk—is terminated under this legislation, there is really nothing to stop them relocating it to a server outside the jurisdiction of this legislation and anyone in Australia with access to the Internet is going to be able to download that content from its new location. So I am not sure what the intention is of this provision and whether people have thought through how it is actually supposed to operate.

Another concern is that, if a telecommunications carrier is supposed to cut off service to someone, that could extend into the family home, in our view, if it is an individual using a phone line or an ISP address to access the Internet. There are other problems with it where there does not seem to be anything to limit their access, for example, to a public service. Many people may, for example, access the Internet through a public library. There may be 40 computers there with Internet access. Could the Attorney give a direction under this proposed legislation to a telecommunications carrier that then flows down to the public library, where all the computers are cut off because someone who is a national security risk has been accessing that public service? Those are the sorts of questions that remain unanswered, and it is our view that not enough effort has been put into considering the practical implications of the legislation.

Senator LUNDY—The department mentioned earlier in their presentation that the bill is designed to shut down whole product suites, if you like, of a given carrier or carriage service provider, which would in fact have the effect that you describe. It would affect far more consumers than actually represent a security risk, by virtue of a vulnerability in the security of the service being provided. Can you respond to the prospect of that occurring?

Mr Murphy—It is a bit like cracking a walnut with a cannon. If there is a minor—or it might be a major—security risk provided by perhaps one individual then the way this is constructed the legislation would allow action to be taken that is like spreading a wide net hoping to catch out the individual, but it is going to affect large numbers of people who do not pose a national security risk. So it is acting in the interests of security but it is affecting many more people than pose the security risk. I think there is a real danger in the way that it is constructed because you could find examples where services are terminated, removed or not accessible for large numbers of people that cannot really be justified. There may in many of those cases be alternative ways to solve the national security problem, instead of having this wide-ranging approach.

Senator LUNDY—Further on that, the Vodafone submission raised the spectre of statutory immunity and the liability that would arise out of such an action if it were taken. Are you in a position to reflect on the impact of that and the potential liability question that could fall to the Commonwealth government if such a directive were given and then a whole group of citizens sought a civil remedy for the damage that that inflicted?

Mr Murphy—I think serious consideration needs to be given in the bill to a process to sort out those issues. There are a couple of problems in this. One is when a direction is given that may affect an individual but some mistake is made in the termination of the service to the individual. Who is going to be liable about that? Is the Commonwealth going to wear a claim by a consumer who has their phone cut off? For example, say a Joe Bloggs is the person whose mobile phone must be terminated and the service terminates the wrong Joe Bloggs, or terminates all the Joe Bloggses who have a service with that phone carrier, in order to comply in the interests of national security? Who is going to be the person who pays any compensation that arises from that?

The other example is when it is more wide-ranging: a service is removed entirely. For example, an existing carrier such as Telstra BigPond might be offering an email service and there may be a need in the interests of national security to terminate that service entirely for a period, resulting in down time for everybody accessing that service. Are consumers in Australia who are not the national security problem required to wear that? Or will it be the carrier or the government?

These are things that should be sorted out in the legislation before it is passed. I think it is unreasonable to be trying to get the courts to sort it out afterwards. It should have a process in place that clearly defines who is going to be responsible and to what extent, and also a process for review. Under the legislation at the moment, while there are avenues in the Federal Court and the High Court, a simple consumer cannot access those, practically or effectively, if some mistake has been made.

Senator LUNDY—Thank you. I am conscious of time. Are there any other points you would like to add before we conclude?

Mr Murphy—I think that covers it. The only other point in our submission was that the bill did not seem to require that existing telecommunications service providers with current licences be subject to security clearance. It just seemed very unusual from our point of view that, if security is the primary concern of this legislation, you would not be subjecting existing carriers to the same process.

Senator LUNDY—Just to follow up that point, this goes back to an issue I raised earlier about what the security standards are, the amount of information available to industry currently to be able to comply and the level of discretion within the national security agencies, defence and so forth to determine what those standards are on an ongoing basis without necessarily advance warning to the industry sector. I am just making an observation there.

Finally, the bill also talks about the power to perhaps prevent the granting of a carrier licence or, effectively, vet both the renewal and the granting of a new carrier licence. Do you have any comments to make about that, beyond what you have already made?

Mr Murphy—If that is the case then there needs to be some clarity in the process—what the requirements are and what the security requirements are for the granting of a carrier licence. It is something that all carriers should be subject to. I think it is unreasonable to be exempting existing carriers from any obligations in that area, yet at the same time suggesting to anyone that wishes to apply for a new carrier licence that there are additional security checks or requirements that they should meet. It seems to be self-defeating. If the security threat is from a carrier then someone could make that threat through an existing carrier in order to avoid proper checks and balances. In order for this proposal to maintain integrity it should be applied to all carriers and all prospective carriers equally.

Senator LUNDY—Thank you.

CHAIR—Thank you, Mr Murphy, for providing your evidence this morning.

Mr Murphy—Thank you for the opportunity.

[12.26 p.m.]

SMITH, Ms Catherine, Acting Assistant Secretary, Security Law Branch, Attorney-General's Department

TEARNE, Ms Anastasia (Anna) Karen Diane, Principal Legal Officer, Attorney-General's Department

CHEAH, Mr Chris, Chief General Manager of Telecommunications, Department of Communications, Information Technology and the Arts

THOMAS, Mr Brenton, General Manager of Enterprise, Infrastructure Branch, Department of Communications, Information Technology and the Arts

WILLIAMS, Mr Don, Section Head of Telstra Shareholder Policy Branch, Department of Communications, Information Technology and the Arts

CHAIR—A few issues have been raised: definitions, such as national security; tightening up the definition of a security risk; the question of judicial review; the question of compensation; and the question of why existing carriers are exempt. Do you have any other issues you wish to raise, Senator Lundy?

Senator LUNDY—Yes, I wanted to find out more about the changes to the information provided from an interception warrant under this bill, and I also have questions that relate back to the definition of national security.

Ms Smith—I will go through the warrant question first. Essentially, what these amendments are doing is purely making it beyond doubt that the current reasonable and necessary assistance that is provided under the Telecommunications Act extends to providing that call associated data, call charge records or billing information that everyone has been talking about this morning when a warrant is executed. A far higher standard is required to get an interception warrant than anything like you need to get information currently under the Telecommunications Act. There is a provision within the Telecommunications Act, off the top of my head it is section 270, which allows a carrier or carrier service provider to provide this sort of information under full warrant. It has been on that basis that this information has always been provided. However, we are not just dealing with the big carriers; we are dealing with small Internet service providers when the law enforcement and national security execute warrants. Often they are not quite clear on their obligations. The purpose of this is to make it beyond doubt that they are required to provide it.

Senator LUNDY—In the context of an interception warrant?

Ms Smith—That is right. To explain, an interception warrant is provided under the Telecommunications (Interception) Act 1979, which is all about protecting our communications which travel over telecommunications systems. This other information is not protected under the Telecommunications (Interception) Act so we could not amend the Telecommunications (Interception) Act because it is information that is protected under the Telecommunications Act, being private information about an individual. My understanding from what law enforcement and national security tell me is that if they just got the call content without knowing who called whom a lot of their intelligence or evidence would be quite useless. I suppose this amendment is just about making it beyond doubt that they can get this

information from the very useful tool that interception is, which has a much higher standard. They could also get this information under other means through a certification process but—

Senator LUNDY—Just to clarify what this bill will enable: at the moment, the interception bill allows the collection of the content of the call—

Ms Smith—That is correct.

Senator LUNDY—and this bill provides for additional information—that is, billing information, time, caller and all that sort of stuff—to be provided at the same time.

Ms Smith—That is correct, but currently the act allows it now under section 270, where you have a lawful warrant. What we are saying is that it is no use providing it at a later date—it needs to be provided at the same time.

Senator LUNDY—But effectively it impacts on that existing power and also on the provisions of the telecommunications interception act, which does protect privacy in a different context. I understand what you are trying to do, but I am trying to understand the impact on other legislation of increasing the power in that way.

Ms Smith—I would say that there is no increase at all in the power. This is purely making it clear in a different provision within the Telecommunications Act that the information should be provided as subject to a telecommunications interception warrant rather than the current provisions—which, my colleague has corrected me, are in section 280—which allows information to be provided under warrant.

Senator LUNDY—And, at the moment, they are two distinct processes under the law.

Ms Smith—No, it is all under one single process. When a warrant is executed upon a carrier as part of delivery of the interception product, they deliver the communication in real time and they also deliver the call associated data. What I was explaining before is that often we are dealing with some new players in the telecommunications industry—smaller ones—and that they just want to know on what basis they should be delivering in real time. They see them as distinct, whereas we are explaining that they are not distinct and they need to be delivered at the same time to assist them in their self-regulation environment.

Senator LUNDY—So you do not really need to make this amendment.

Ms Smith—That is right. It is to assist industry in meeting their obligations.

Senator LUNDY—So, to play devil's advocate, why don't you just put out a guidance note saying, 'This is how you do it under these powers'?

Ms Smith—We do do that. The trouble is that the industry is getting so large. The difficulty with dealing with new players all the time is that they have often gone to the legislation as the first point before we hear from them, and they will put their practices in place. What we want is that, in developing their new services, they actually put these things in place initially. That is quite correct: we could put some general information out to everyone in the industry.

Senator LUNDY—Regarding the privacy issues relating to call data disclosure, I understand that in the context of a warrant they do not have a place but, in the absence of an interception warrant, what implications do these changes we are discussing have?

Ms Smith—I think the only change—and please correct me if I am wrong—regarding the release of information is to change the definition of a senior officer. That is the only change in relation to this. The current protections to your personal information in the act are still there. It can only be released where either the carrier or the law enforcement agency is satisfied that there is a belief that the person is engaging in a criminal offence, or the protection of the public revenue—

Senator LUNDY—They are existing offences.

Ms Smith—Yes, they are the existing thresholds for releasing the information.

Mr Cheah—In section 282.

Ms Smith—In relation to the provisions relevant to national security in section 283, the only change is the definition of ‘senior officer’.

Senator LUNDY—Going from what to what?

Ms Smith—We had been told by the agencies that the definition of ‘senior officer’ meant that in many agencies only one or two people at a very high level could sign off on certifying that this information was needed for the enforcement of criminal law, because the nature of a lot of agencies has changed—we now have a lot of anticorruption commissions that do not have the normal police structures and things like that. So we have amended the legislation to reflect the new structures within those organisations. It is no watering-down legally.

Senator LUNDY—Is that a long way of saying that more people can tick off?

Ms Smith—No, not more people—although I suppose it is in the long term, because the number of those who could do it was dwindling because the definition did not apply to these organisations.

Mr Cheah—The current act says that a senior officer in an enforcement agency—these are the people who can currently do it—is, if the agency is a police force service, a commissioned officer, and some of the police forces do not necessarily have commissioned officers in the same way; or, if the agency has a senior executive service, however described, a senior officer is an officer of that service, and some of them do not have SESs any more. So the trouble is that some of these definitions on which it worked no longer exist, and these were the only categories in which you could have somebody issuing the relevant authorisation. What we are now saying is effectively that the CEO of the law enforcement agency determines that a person is of sufficient seniority to be able to exercise this particular power. But it is quite clear that they have to be a senior officer and a person who is—

Senator LUNDY—But it is up to the CEO to determine that. How can you say that that is not a watering-down of the act?

Mr Cheah—Because I think it is fairly clear that it has to be a senior officer. The CEO has to make a call that the person is of sufficient seniority to exercise these discretions.

Senator LUNDY—I am not going to debate it here, but it seems pretty loose to me. Are we talking about the release of information that would otherwise be covered by the privacy aspects and provisions in the absence of an interception warrant?

Ms Smith—That is right.

Senator LUNDY—Going through the list Senator Eggleston identified, we heard very strong submissions from Vodafone and from the civil liberties council that the definition of national security is still way too broad and certainly has not created an understanding of what is required, at least for those two submitters. What is your response?

Ms Tearne—As I mentioned earlier this morning, both of the provisions that are contained in the bill with regard to directions on security matters make reference to the fact that security in the context of those provisions has the meaning given in the ASIO Act, and that act defines the concept of security. It defines it by reference to a couple of topics, amongst which are politically motivated violence, attacks on Australia's defence systems et cetera, but it certainly defines the concept and those terms are each further defined within the definitions contained in the ASIO Act. So there is a concept of security. It is defined in the ASIO Act and that definition is picked up in the bill we have before us. I think Cameron Murphy raised concerns in relation to environmental protests, trade union activity and the like.

Senator LUNDY—Consumer groups.

Ms Tearne—Consumer groups et cetera—just as a few examples. I would not envisage that the ordinary activities of those organisations would transgress what are defined as the heads of security and engagement in activities that are prejudicial to those areas of concern. Moreover, the ASIO Act in itself sets out that this act is constrained by the fact that matters of lawful advocacy, protest or dissent and exercise of those rights shall not be regarded in and of themselves as being prejudicial to security, and the functions of the organisation—which include the provision of security assessments—are construed accordingly. So there is some protection by the fact of picking up the definition of security contained in the ASIO Act.

Senator LUNDY—Chair, it would be interesting to convey that to both the submitters and see if we can get some feedback from them.

CHAIR—We can get a copy of the ASIO Act, no doubt, and include that section in the report.

Ms Tearne—Certainly. Section 17A is the reference to lawful dissent et cetera. The definition of 'security' is contained in a rather long section which contains a number of definitions. I believe it is section 4 of the act.

Senator LUNDY—Do those definitions under the ASIO Act, given they have such relevance to what we are discussing today, also cover those types of activities occurring in a virtual environment—in a digital environment—and the incarnation of those activities within a telecommunication service?

Ms Tearne—The act itself does not draw technical distinctions in terms of the environment in which those particular security concerns may arise but—

Senator LUNDY—I know, but the Telecommunications Act does.

Ms Tearne—if I take that a little bit further, those heads of security are defined by reference to types of conduct. That conduct could theoretically occur in a number of environments. Whilst politically motivated violence might be an act of physical violence, potentially it might be enacted by other means. But I could not comment in terms of creating hypothetical examples, but certainly it would not limit itself to physical conduct.

Senator LUNDY—So your understanding of it is that those exclusions would extend into the digital environment.

Ms Tearne—The definitions?

Senator LUNDY—The definitions. Is it reasonable to describe that definition as ‘exclusions’?

Ms Tearne—No, it is an inclusive definition and the term ‘security’ is defined as ‘the protection of ... the Commonwealth and the several States and Territories’ from those particular types of activities. So they are not really exclusions but perhaps an inclusive definition of what constitutes security.

Senator LUNDY—So there are some positive examples and some examples of what would not be included?

Ms Tearne—It sets out what would be included and then each case would be assessed against those particular heads to determine whether the particular conduct was something that was—

Senator LUNDY—You read out a list of things that would not have been included.

Ms Tearne—Yes, that is a qualification that applies generally in relation to the act and functions of the organisation, which says:

This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly.

Senator LUNDY—I have a general question but I do not know whether you will be able to answer it. One of the features of the Internet, for better or worse, is that it is a platform and a vehicle for the sharing of information. I can think of a number of scenarios where sensitive information that could arguably affect national security has been disclosed, leaked or otherwise—and I am thinking of the Drudge report and others in the US—where public information that had a classification was released and published. Would the disclosure of sensitive information like that initiate a proceedings and a directive under this bill that we are discussing?

Ms Tearne—The answer to that is that disclosure of sensitive information is already the subject of other legislation on the Commonwealth statute books. The Crimes Act is just one example in terms of the disclosure of sensitive information or information that—

Senator LUNDY—Under national security grounds there are existing laws that could cover that?

Ms Tearne—I am not in a position to say whether it would extend; I would envisage that the mechanisms for dealing with the disclosure of information would be mechanisms other than those proposed in the current bill.

Senator LUNDY—So my question is: is there another act that would cover that on national security grounds? Or would this be the only piece of legislation that could conceivably address that sort of disclosure—on national security grounds, as opposed to a raft of existing laws?

Ms Smith—I understand there is an ALRC reference at the moment that is looking at classified information and the disclosure of such. I am not clear on their terms of reference but I am quite aware that they will be reporting early next year. They are looking at quite a broad area of this whole disclosure of information, which is currently only allowed for in very small provisions in the Crimes Act at the moment. Going back to the whole purpose of this amendment, it is really about ASIO's ability to execute a warrant that has been issued. It is where there is a risk to national security by executing that warrant on a particular individual—that it is more what it is about. I do not think—

Senator LUNDY—I appreciate that. I know we have gone into areas that could be described as having unintended consequences, but that is the purpose of these inquiries.

Ms Smith—Certainly, but I would not see that that was the intention or the ability under this bill.

CHAIR—Vodafone also raised issues about the definitions in terms of the need to amend section 581(3)—so the power under 581(3) can only be exercised:

... where there are demonstrated grounds that this is necessary to protect national security and only where risk to national security cannot be managed effectively through other mechanisms.

They are seeking to have a more specific wording there. What is your comment about that?

Ms Smith—I think what they have said is the actual intention of what exactly will be done. We will need to demonstrate to the Attorney-General, the Prime Minister and the Minister for Communications, Information Technology and the Arts that these risks do apply. But the difficulty with disclosing that information generally, because it would potentially disclose national security information—

Senator LUNDY—It would expose the vulnerability.

Ms Smith—That is correct. So we would be against a provision that required any public disclosure. What was the next part of your question?

CHAIR—I suppose what I was saying by implication is that there would be demonstrable grounds, which the Attorney-General would know about, but they would not necessarily be able to be made public.

Ms Smith—In this earlier process—before it gets to that extent—there will be consultation. Certainly, Vodafone were not sure, in relation to this bill, what the level of consultation would be. They will know about it if we have concerns that there is vulnerability within a particular service that they are providing or a particular group that they are providing it to. There certainly would never be any surprises and that is where we would endeavour to consult and talk about perhaps removing the visibility of a particular area to particular parts within their organisation and that sort of thing. There is a determination under part 15 of the Telecommunications Act whereby the agency coordinator can require a particular carrier to describe how they will protect the national security and law enforcement information that is provided to them. It is that kind of process we would envisage that will highlight to them that we have a concern. We will look at what they have to say and try to address it and only in rare and extreme circumstances go to the point of having the Attorney-General make a direction.

Senator LUNDY—What has come out is that the current drafting of the bill is so broad it has generated the spectre of all these other scenarios that you have told us today were not initially envisaged. You have told us that the bill is supposed to relate to the government's ability to ensure that the Telecommunications (Interception) Act can operate efficiently and effectively.

Ms Smith—That is correct.

Senator LUNDY—I have a series of specific questions I want to move through in the time available. The first one relates to the potential impact on competition in telecommunications. What is the distinction between the treatment of new and existing carriers under this bill and has there been any thought given to the impact on the theoretical competitive environment in telecommunications on the basis of security standards or expectations and security management issues?

Mr Cheah—I will answer the second question first and then I will pass back to my colleagues in the Attorney-General's Department for the first question. The communications portfolio has been involved in the drafting of this bill. We are very comfortable with it in terms of that it is, from our point of view, really only buttressing some of the existing provisions in the existing policy and basically providing a way of dealing with specific problems when they arise.

We think it has some pretty significant safeguards in there in the sense that the Attorney will not just be exercising his powers to shut down a particular service unless he has consulted with the minister for communications. At the end of the day, the Prime Minister must be involved—we had that discussion before. Overall, we think that there are no competition problems at all from the bill; it is basically level playing field stuff.

Senator LUNDY—Is there different treatment of existing and new carriers under the provisions of the bill?

Ms Smith—No, essentially the bill is allowing us to get in under the legislation at an earlier point. The current practice is, in fact, that the Australian Communications Authority advises us when a carrier's licence has been lodged and then gives an opportunity to make contact at that point. All of those processes that are currently in place with the carriers—and I suppose this gets to a standards question—do actually have some standards in relation to telecommunications interception. We provide technical standards for what we require—auditing standards and access standards—and we apply the *Commonwealth Protective Security Manual*.

In our negotiations with the current carriers, we require them to meet all of those objectives when they provide interception capability. Probably 99 per cent of the consultation before issuing a carrier's licence is to get in early and make them aware of obligations, and we can be aware of any concerns and that sort of thing. Then, with that one per cent, if there are any concerns on national security grounds we can try and manage those. We already have management processes in place with some existing carriers that have licences, where we have asked them to protect national security information and law enforcement security information away from their general management structure when we have been concerned that there may be national security concerns. Of course, there is a distinction because this legislation—if it

comes in—will only apply to new carriers licences, and there are already about 90 out there. But the way that we deal with them on a daily basis will be identical.

CHAIR—That is the point that the *Bills Digest* makes. It says:

... security clearances will be required for new telecommunications carriers but not for companies with existing carrier licenses.

but you, in effect—

Ms Smith—That is actually not correct. A security assessment will only be done when we have got to the point where we think that there is potentially a risk to national security. There may be information that has come to light—from ASIO doing their everyday work—that has identified a particular individual, a particular organisation or something like that. In that case, the security assessment will progress. But, on a general basis, I think it is fair to say that 99 per cent will just go through without any security assessment.

CHAIR—The *Bills Digest* also expressed concern about the length of the consultation period which, for licence carrier applications, is up to 12 months.

Ms Smith—Yes. The initial consultation is only 15 days before we have to invoke the extension of time. The Australian Communications Authority, when we consulted with them at length, were very concerned about this. They wanted to put only five days on us, which was a physical impossibility—

CHAIR—Sorry?

Ms Smith—They wanted to shorten the period of time, but it was a physical impossibility for us to consult in that time. For example, we may need to consult internationally or all around Australia—we consult with 11 intercepting agencies on a daily basis. So we felt that 15 days was a period of time where we could turn most over; those that we cannot will be the exceptional cases.

CHAIR—All right.

Mr Cheah—Once again, from the communications portfolio perspective, we are very comfortable with that. The way we see these provisions operating is that the national security apparatus basically has 15 days to put their hands up and say, 'We think we might have a security problem here which we need to investigate.' With the time period that they have, the ASC can continue to process the application. If the hand does not go up, it does not blow out in any way. It reverts to 28 days which is, I think, the normal time period for which a carrier licence would have been granted under the previous rule.

Basically, the only time when you are going to get the clock stopped is if the national security machinery thinks that there might be a problem. But, once again, there is still no guarantee that there will be. Just returning to your original question, Senator Lundy, and the differences between existing carriers and new carriers, there might be a theoretical distinction between the two, but in practice we do not think there is seen to be a problem with the existing 90 carriers. This basically provides a mechanism for identifying future risks as they come into the system, but we are not expecting too many of those.

Senator LUNDY—You said that in the preparation of this legislation you did consult with carriers.

Mr Cheah—Yes, carriers were involved. I think we mentioned the names of five carriers. They were the biggest five: Telstra, Optus, Vodafone, Hutchison and AAPT.

Senator LUNDY—Can you tell me if you have consulted with any smaller carriers or carriage service providers, given their technology may be different and they may be less capable to provide the information necessary under the interception act? Have you done a comparative analysis of the impact of this bill on smaller carriers?

Ms Smith—We are not actually placing additional obligations on any of the industry as part of this legislation. Certainly we are dealing with the small carriers. At the moment we are dealing in a big way with all of the broadband wireless providers and explaining to them all the capabilities. I think it is important to note that the act actually provides for an exemption regime, which we are tightening up under the legislation. That tightening up, I should point out, is on us, in our office—that we have to turn them around within 60 days. That will allow that if it is a small ISP which does not have the target market that is of any interest to law enforcement, where there is no possibility that they can provide such a capability, they will get exemptions. We practise this on a daily basis in dealing with the small as well as the large. As far as the consultation regime is concerned, even though, for example, Telstra provides fixed line services as a main service, their BigPond is one of the major ISPs. So they actually do represent ISPs, sit on ISP consultation bodies, and pass on a lot of information to the smaller players.

Senator LUNDY—I am also very conscious that the sector is extremely competitive, and the capabilities and technological set-up of the bigger players might vary significantly from the smaller players. I would be concerned if this bill was constructed in recognition of the environment as expressed by the bigger players without taking into account the impact on some of the smaller players.

Ms Smith—No, certainly they represent a full interest. We are constantly concerned about the cost of competing in this environment.

Senator LUNDY—Have you been talking to other ISP groups and industry associations?

Ms Smith—We deal with the Internet Industry Association.

Senator LUNDY—What about the other ISP groups, like the Internet Society of Australia, which represent smaller ISPs?

Ms Smith—They have not been involved in any of the forums that I have been at. There is consultation in other areas.

Senator LUNDY—Perhaps I could ask DOCITA.

Mr Cheah—The way the bill works is that all of the operative provisions come in when somebody wants to become a carrier. So it is basically when you start getting seriously involved in infrastructure. Our view has been that there is nothing in this legislation which imposes any particular additional substantive barriers in the way of people getting a carrier licence.

Senator LUNDY—Or participating in the market.

Mr Cheah—Or participating in the industry or anything like that. We have not gone to the wider group, really. Most of the reason for consultation would have been just to make sure

that there was nothing in some of those other changes we were making which were going to cause us a problem, because we did not regard entry proposition as being an issue.

Senator LUNDY—You mentioned security assessments before. They are, presumably, done by a security agency. Would that be ASIO?

Ms Smith—Yes.

Senator LUNDY—In the process of conducting a security assessment, are there standards and guidelines available to carriers to inform them what it would involve? I guess what I am looking for is a mechanism that would allow carriers to prepare for such an assessment, to take into account the problems and issues that ASIO are legitimately concerned about and trying to address.

Ms Tearne—I think the answer to that is essentially no, there are not guidelines that would be available to carriers to prepare for a security assessment as such. However, the function of preparing for security assessments is one that is set out in the ASIO Act. It does set out exactly what constitutes a security assessment, the effect that it has and of course that the security assessment is referable back to the functions of the organisation and the heads of security. So to that extent anybody in the Australian community is on notice that those are the issues with which the organisation is concerned and that those are matters on which the organisation may furnish the Commonwealth with an assessment on.

Senator LUNDY—What safeguards are in place to demonstrate to an average Australian consumer, who may or may not be the subject of investigation, that they will not have their phone connection cut under the measures contained in this bill solely? If they are under investigation, is there an additional national security benefit being derived from this bill that goes beyond what already exists in ASIO's telecommunications interception powers?

Ms Tearne—I suppose I could take it back to the initial question in terms of safeguards. A number of safeguards are available and some of them come back to the provisions in the current bill and some of them come back to safeguards in place in the security assessment regime in the ASIO Act. We would see some of the safeguards in the communications bill as being the very high threshold that has to be met in terms of the Attorney-General being satisfied that the use of the service would be prejudicial to security—likewise, the consultation at a very high level with the Prime Minister and the minister for communications.

As I mentioned previously, security assessments are reviewable on their merits by the Administrative Appeals Tribunal. So there is a process in place—and it has been in place for quite some time—for reviewing assessments exactly of this type and that has been used quite successfully, as I understand it, in a number of cases and other contexts in which security assessments are issued. So there is a variety of different safeguards at a number of different levels. Taking it to an even higher level of generality, in terms of the preparation by the organisation of security assessments, the organisation itself is subject to a number of oversight mechanisms, not least of which is answering to its minister but also the Inspector-General of Intelligence and Security, who is an independent officeholder. So I suppose there is a range of mechanisms. I can go into some of those in more detail if you like.

Senator LUNDY—Can you encompass for the committee what benefit this bill will provide for national security that is not already covered in existing powers and legislation? Is it really just about hitting the carriers over the head saying, ‘You have to do better in providing this interception information’?

Ms Smith—I suppose it is about satisfying that a national security agency and law enforcement agency can go forward and execute a warrant upon on a particular carrier or carriage service providers and know that they will receive the appropriate product and the necessary information with that, and be satisfied that the information they are providing to that carrier, which is highly sensitive information whether it be for a national security reason or criminal law enforcement, would be sanitised from the rest of the operations of that organisation and protected so that their investigation would be in no way compromised. I think that is essentially the purpose and the hope this amendment will give them—surety of a system that will mean all of the information is protected and on the other side of the coin, and I think Peter briefly said this this morning, that citizens are satisfied that our communications are not being unlawfully intercepted. Many years ago there were amendments to make it that a carrier itself could not listen into calls except for very narrow and technical reasons. So it is about ensuring that if there is a concern that there is someone listening in and there is a threat to a national security then that can be stopped.

Senator LUNDY—Can you explain a scenario or a situation where national security would benefit from a directive to disconnect a phone service rather than ASIO intercepting a phone conversation and acting on the intelligence obtained from it?

Ms Smith—No, I cannot. It was not the intention of this legislation so we have not actually looked at that as being a benefit.

Senator LUNDY—Removing names and other identifying attributes, can you provide examples of occasions in the past where Australia’s national security has been placed at risk because the Attorney-General was unable to disconnect a phone service?

Ms Smith—No, I cannot.

Senator LUNDY—You have now said that the purpose of this law is not to provide a power to allow the Attorney-General to direct a disconnection of a service—

Ms Smith—Of an actual service, yes, or an individual service.

Senator LUNDY—or an individual service, so are you able to assure the committee that these laws will not be used to prevent individuals or groups from using Internet services?

Ms Smith—The laws as they stand may prevent a carriage service being provided, which may inevitably prevent an individual who might have wanted to use that service from accessing it. They may have to go to another service provider for a particular service. As far as targeting individuals goes, I am not sure whether I can actually answer that question.

Senator LUNDY—My understanding from what you have told me is that the intent of the law is not that it be used to prevent individuals or groups from using Internet services or services on telecommunications carriers.

Ms Smith—No, that is right. It is protecting the actual service or the infrastructure.

CHAIR—The only other broader issue that was mentioned was this question of judicial review. The *Bills Digest* felt that there were some limitations in that, if the Attorney-General genuinely considers that the grant of a carrier licence or the use or supply of a telecommunications service would be prejudicial to security, there would be little prospect of a successful application for judicial review. In other words, if the Attorney-General makes that finding then it is difficult to obtain judicial review. What do you say to that?

Ms Tearne—I suppose there are two different aspects to that question: first of all, the question of seeking judicial review and second of all, the general availability of review of whatever type in relation to those decisions. To start by reference to the review that is available, the bill does exclude the decisions made under proposed sections 58A and 581(3) from the review mechanisms that are set out in the Administrative Decisions (Judicial Review) Act. It then substitutes, in place of that mechanism, the mechanism that is available in respect of the review of security assessments under the ASIO Act, which is a tailor-made statutory framework for the review of decisions in which there are security aspects. The very simple reason for that is that the Administrative Decisions (Judicial Review) Act framework is not one that is designed to cater for security type issues, whereas the Security Appeals Division has some very specific provisions in the AAT Act that allow for protection of sensitive information and make that forum a much more appropriate one for review of these types of decisions.

CHAIR—How accessible is that?

Ms Tearne—My understanding is that it is quite accessible. It has been used on a number of occasions. Certainly the organisation as it stands has a function of providing security assessments in a range of contexts, the most common of which is designated security assessment positions within the Commonwealth—persons who need to hold security clearances to do their work for the Commonwealth. The organisation also conducts security assessments in a range of other contexts identified in the act. The AAT review mechanism has been used to review those decisions. I am not in a position to comment on the time that the AAT might take or the cost of that, but my general understanding is that it is quite accessible and low cost.

Senator LUNDY—Mr Chair, may I suggest that, because so many of the issues that have been drawn out in this bill relate to the definitions contained in ASIO Act and associated legislation, there might be an opportunity for this committee to discuss this bill with the other Senate committee on those issues, or something along those lines?

CHAIR—We will consider that on Monday when we talk to other people.

Senator LUNDY—I am very conscious of the fact that I do not have the level of familiarity with the ASIO Act that I think is necessary for a deeper understanding of the implications of this bill.

CHAIR—Okay, that could be considered.

Senator LUNDY—Thank you.

CHAIR—The other general issue is the issue of compensation, but I think that is really a policy issue and not one that you really should have to express views on.

Ms Smith—I think the only comment I would make is that the doctrine of frustration will apply in relation to any carrier's direction to cease to provide a carriage service. There needs to be a distinction made between the provisions under 313 and 315 that Vodafone talked about. In those cases, they have discretion to do certain things; in this case, they will not have discretion. I assume on that basis that their contracts would be frustrated but, in the other cases, they are certainly making decisions based on their own interpretation.

CHAIR—As there are no more questions, we will conclude this hearing. I thank you all for appearing. We have a reporting date of next Tuesday, but we will seek to have that reporting date extended.

Committee adjourned at 1.11 p.m.