COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

Reference: Telecommunications (Interception and Access) Amendment Bill 2007

MONDAY, 16 JULY 2007

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

SENATE STANDING COMMITTEE ON

LEGAL AND CONSTITUTIONAL AFFAIRS

Monday, 16 July 2007

Members: Senator Barnett *(Chair)*, Senator Crossin *(Deputy Chair)*, Senators Bartlett, Kirk, Ludwig, Parry, Payne and Trood

Participating members: Senators Allison, Bernardi, Birmingham, Boyce, Bob Brown, George Campbell, Carr, Chapman, Cormann, Conroy, Eggleston, Chris Evans, Faulkner, Ferguson, Fielding, Fierravanti-Wells, Fifield, Fisher, Heffernan, Hogg, Humphries, Hurley, Joyce, Kemp, Lightfoot, Lundy, Ian Macdonald, Sandy Macdonald, McGauran, McLucas, Milne, Murray, Nettle, Patterson, Robert Ray, Sherry, Siewert, Stephens, Stott Despoja, Watson and Webber

Senators in attendance: Senators Barnett, Kirk, Ludwig and Parry

Terms of reference for the inquiry:

To inquire into and report on: Telecommunications (Interception and Access) Amendment Bill 2007

WITNESSES

Committee met at 2.03 pm

CHAIR (Senator Barnett)—I declare open this hearing of the Senate Standing Committee on Legal and Constitutional Affairs in its inquiry into the provisions of the Telecommunications (Interception and Access) Amendment Bill 2007. The inquiry was referred to the committee by the Senate on 21 June 2007 for report by 1 August 2007. The bill amends the Telecommunications (Interception and Access) Act 1979 and several other related acts to implement further recommendations from the August 2005 review of the regulation of access to communications by Anthony Blunn AO. The committee has received 24 submissions for this inquiry. All submissions have been authorised for publication and are available on the committee's website.

I remind all witnesses that in giving evidence to the committee they are protected by parliamentary privilege. It is unlawful for anyone to threaten or disadvantage a witness on account of evidence given to a committee, and such action may be treated by the Senate as a contempt. It is also a contempt to give false or misleading evidence to a committee.

The committee prefers all evidence to be given in public, but under the Senate's resolutions witnesses have the right to request to be heard in private session. It is important that witnesses give the committee notice if they intend to ask to give evidence in camera. If a witness objects to answering a question the witness should state the ground upon which the objection is taken and the committee will determine whether it will insist on an answer, having regard to the ground which is claimed. If the committee determines to insist on an answer, a witness may request that the answer be given in camera. Such a request may of course also be made at any other time.

[2.03 pm]

BURGESS, Mr Mark, Chief Executive Officer, Police Federation of Australia

CHAIR—Welcome. Thank you for being here. The Police Federation has lodged its submission, No. 4, with the committee. Do you wish to make any alterations or additions to the submission?

Mr Burgess—Not to the submission itself.

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

Mr Burgess—Thank you for the opportunity to appear here today on behalf of the Police Federation of Australia, which represents the professional and industrial interests of Australia's 50,000 serving police officers. As we have outlined in our submission, we strongly support the current and proposed provisions in the bill, which enable the use of telecommunications intercepts, stored communications and telecommunications data for the enforcement of the criminal law, including against corruption. However, we are concerned that the proposals in the bill in respect of secondary disclosure provisions will mean that police officers, simply due to their occupation, will have a lesser standard of rights with respect to privacy than other workers and citizens in general.

As our submission highlights, our key area of concern with the bill centres around the proposed new section 182(2) dealing with secondary disclosure or uses offence. This section will allow the disclosure and use of telecommunications data against police officers in non-criminal actions, such as disciplinary proceedings, and this will be achieved by using the terminology for the enforcement of the law imposing a pecuniary penalty. It is this provision which is likely to impinge on the area of police disciplinary proceedings, as the disciplinary offences applicable to most police jurisdictions are found within state and territory legislation and have provisions for pecuniary penalties by way of fines even for very minor matters. We accept that along with extensive powers conferred on police comes greater accountability. However, you would be aware that each jurisdiction already has in place a variety of mechanisms to ensure such accountability. As it is, police officers perform difficult and stressful roles and are subject to significant internal and external disciplinary proceedings and oversight arrangements in the event that an individual error of judgment or misdemeanour occurs, or workplace behavioural issues need to be dealt with.

We have provided the committee with correspondence from the Attorney-General to the PFA dated 28 May 2007 in response to our concerns. It is our interpretation of his letter that any impact of this bill on police disciplinary matters is an unintended consequence of the proposed legislation. That being the case, we urge the committee—

CHAIR—Was that a quote?

Mr Burgess—No, that is not a quote.

CHAIR—That is your advice?

Mr Burgess—Yes. That is our interpretation of the letter.

CHAIR—Thank you.

Mr Burgess—Any impact of this bill on police disciplinary matters is an unintended consequence of the legislation. That being the case, we urge the committee to investigate options that will support the intent of the bill but alleviate our concerns that minor police disciplinary matters will be caught up in the secondary disclosure provisions. We have proposed one possible amendment to the bill and will be happy to work with the committee to explore other options that may give comfort to our concerns but at the same time meet the intent of the bill.

CHAIR—We appreciate your evidence.

Senator LUDWIG—Do you have a copy of the Attorney-General's letter before you?

Mr Burgess—I do.

Senator LUDWIG—Turn to the third paragraph, which begins 'As you may be aware'.

Mr Burgess—Yes.

Senator LUDWIG—It then relates to disclosure of telecommunications data, and then in the penultimate paragraph it states:

A secondary disclosure of telecommunications occurs when the recipient of the primary disclosure passes that information on to another body.

Putting that together with the second paragraph on page 2:

The new legislation would not alter the threshold ... In other words, this permits the secondary disclosure of information to an agency in circumstances where the receiving agency would itself have been able to access the information directly from the carrier.

Do you understand generally what the term 'telecommunications data' would include?

Mr Burgess—The explanatory memorandum gives me some idea what he was talking about.

Senator LUDWIG—There is no definition of 'telecommunications data' in the bill itself, though?

Mr Burgess—No.

Senator LUDWIG—If we rely on at least that, with respect to the secondary disclosure of information, your concern would be that if it was a chapter III court it would be limited but if it is not a chapter III court—that is, it relates to tribunals and so on—it could include ordinary disciplinary matters that your members may be subject to.

Mr Burgess—That is in essence our concern. In the letter from the Attorney-General, in the third last paragraph on page 2, he states:

This is by reason of the meaning of 'pecuniary penalty', which is limited to specific monetary penalties set out in relevant legislation and imposed by a court.

As I indicated in our submission, most of the legislation in respect of the disciplinary issues for police officers is contained within various pieces of legislation in the states and territories with respect to police acts and police discipline, and in each of those they deal with how they may be dealt with, such as tribunals, appeals courts and even hearing officers, which we

would suggest would potentially come under the definition of a court. Therefore, that leaves us with a concern that very minor matters that potentially carry a financial penalty could be caught up in this bill.

Senator LUDWIG—The letter then states, at the bottom of page 2:

Nor will they permit the general use of telecommunications data in police disciplinary proceedings, either on the basis of a primary or secondary disclosure.

Does that not give you comfort?

Mr Burgess—No, it does not.

Senator LUDWIG—Why is that?

Mr Burgess—We are concerned that the bill will give the ability to disclose information, as limited as it might be, which will therefore allow people to undertake fishing expeditions for further information that they might think they can gather, and when they might not have been aware of any of this in the first place. This is not about preventing appropriate use of this legislation or this bill to target police officers undertaking criminal or corrupt activities. Our concern centres around the prospect of it being used in respect of what all of us in this room would consider to be minor disciplinary issues. Because the relevant legislation that underpins those disciplinary issues has provisions for monetary penalties, they will be picked up.

Senator LUDWIG—Have you considered how the bill could be altered to accord with your view or the Attorney-General's view that 'the general use of telecommunications data in police disciplinary proceedings, either on the basis of a primary or secondary disclosure' should not be permitted?

Mr Burgess—We have suggested in our submission—and I would be guided by the expertise of the committee as well—that to delete the amendment would cause some concern. But we have talked about trying to clearly define what you mean by a 'court', which might exempt those issues around disciplinary proceedings, such as appeals boards, tribunals, hearing officers or the like, so that you would not find those minor disciplinary issues being swept up by this. This goes back to our original proposition. Our reading of the Attorney-General's response is that he does not know that those issues would be clearly picked up. In fact, he says that our concerns are only partially correct. Our interpretation is that, if we are correct, this is an unintended consequence of the legislation.

Senator LUDWIG—What types of disciplinary proceedings are contemplated by you when you say that they would be captured? Can you provide an example of those?

Mr Burgess—In virtually all of our jurisdictions with the exception of a couple, there is provision for a fine for the most minor matter. An example would be insubordination or someone speaking inappropriately to a motorist. All of those matters are potentially subject to a fine. In essence, it is a case of how long is a piece of string as to what issues are picked up in this piece of legislation.

Senator LUDWIG—How is that regulated?

Mr Burgess—Under the various state—

Senator LUDWIG—The state policing legislation that applies?

Mr Burgess—Yes. It is also our understanding that the Attorney has said to some people—and it has not been said to us—that perhaps we should look at the respective state acts to take out a notion of pecuniary penalties. Whilst that would be a worthwhile objective, it certainly would not be simple to have those six or seven other pieces of legislation potentially amended so that there is no impact on this particular bill.

Senator LUDWIG—You would be unaware of whether you would gain support from the commissioners of the relevant policing—

Mr Burgess—Therein lies the difficulty. It would be a big exercise to go down that road. Whereas what we are suggesting is that, if it is not the intent of the legislation to pick up those matters, then let us make it clear. If it is about criminal matters, et cetera—those serious types of matters—let us make sure that that is what we are talking about. We need to make that clear. If it is not about minor matters of police discipline, we need to make sure those things cannot be picked up in the bill.

Senator PARRY—Can you give us an example of what you think might be picked up with respect to the passing on of secondary information? I have been racking my brain to think of a practical example. Would you be able to provide a scenario that you think would fit?

Mr Burgess—I have not turned my mind to an example. I am sure with your policing background you can probably imagine that somewhere along the line someone will. I will use the ATO as an example, because it is an outside agency. It could be investigating a tax agent for matters in respect of tax law. There might have been some contact between a police officer and the tax agent about something unrelated to the criminal offence but potentially related to something the officer may or may not have done in their role as a police officer, and this alerts the ATO to the fact that this is something that should be passed on to the respective police department. It need not be a criminal matter and it need not be involved in the ATO investigation. However, it might give rise to a police disciplinary matter. As minor as it might be, this potentially gives the ATO the authority to hand that information on to the respective police department.

Senator PARRY—Would not the ATO have a policy within its charter of not passing on information that is not directly related to the original investigation? If you are dealing with a third agency, I would have thought there would be other protocols in place.

Mr Burgess—I do not know whether or not there are.

Senator PARRY—It is hard when we are talking hypothetically.

Mr Burgess—The proposed legislation would in fact allow them to do that if they so desired. It could be another police agency. It is the same thing.

Senator PARRY—The potential is there?

Mr Burgess—There are no arguments about investigating someone for a criminal offence. We are not arguing about that. But if something else comes to light that is not criminal from someone in another jurisdiction, is there then a compulsion on them to hand over that information as minor as it might be?

Senator KIRK—I wanted to go back to the definition of ‘court’, because that seems to be critical here. You say in your submission that it ‘should be defined as a legally constituted

criminal or civil court over which a judge or magistrate presides.' Would you want it to extend to civil courts as well? The thrust of what you have been saying is that it really should be in relation to criminal matters.

Mr Burgess—Again, I stand to be corrected, but my understanding of the definitions in the bill is that this would apply where pecuniary penalties were applicable. A civil court would be picked up in this definition. What we are trying to do is differentiate a police disciplinary arrangement from a criminal or civil court.

Senator KIRK—Are you happy with disciplinary matters that might take place in a civil court? Are you just trying to distinguish between disciplinary tribunals and courts?

Mr Burgess—Yes.

Senator KIRK—In a more general sense, what do you see as the practical difference between the way telecommunications data is currently dealt with and the new arrangement that is being proposed, in practical terms?

Mr Burgess—We have tried to keep ourselves concise on this particular issue—

Senator KIRK—Just on the disclosure.

Mr Burgess—as opposed to the bill in its generic terms. In essence, all I am saying is that this new provision changes the ball game in that respect, in that this data could now be handed over where it might relate to a disciplinary offence. That would be a matter that would ultimately have to be tested, but the data could be handed across.

Senator KIRK—Of course, you would like to see the amendment deleted but, failing that, could this be solved by narrowly defining 'court' so that it excludes these other matters?

Mr Burgess—We are not about preventing the bill from going forward.

Senator KIRK—I understand that.

Mr Burgess—We are not arguing about the bill in its generic sense. We are concerned about that one small aspect of it, which obviously is subject to debate. In his letter, the Attorney-General said that our concerns are only partially correct. We could have a debate about that. Somewhere along the line that will be tested and will either be found to be right or wrong. All we are saying is that it is not the real thrust of the bill to chase police who may or may not have been involved in a disciplinary matter. The real thrust of the bill is far greater than that. Aside from the part about which we are concerned, we are not arguing about the rest of the bill.

Senator PARRY—Were we to delete proposed section 182(2)(c), which is the issue that you are concerned about, what gap would be created in the legislation? That might be substantial. I am of the view that it is a state issue. You might have to get state commissioners or state ministers to change the legislation. Again, I cannot think of a strong example of how police are going to be caught up in this from a practical perspective. I know the potential exists.

Mr Burgess—As I said, we talked about the two options, including deleting that section. I do not know what sort of hole that would leave in the bill. It might be substantial. We are not trying to do that. However, we are trying to prevent this particular issue. Were we to raise an

example today, people can say that that is not likely to be the case. But having been around long enough, as I am sure you have, I know somewhere down the line it will be tested.

Senator PARRY—That might be for good merit, but we do not know. Apart from proposed section 182(2)(c), is the bill fine?

Mr Burgess—Yes. We have not raised any other particular aspects or concerns.

CHAIR—You have all of us thinking about your suggestion or proposal for a possible amendment. I am looking at proposed section 182(2)(c), which we have been referring to. The explanatory memorandum cites an example regarding the tax office:

… if during the course of an investigation in relation to taxation fraud, the Australian Taxation Office obtains telecommunications data that concerns drug trafficking, the Australian Taxation Office could lawfully disclose this information to a relevant police agency to investigate.

You do not have any problems with that type of situation?

Mr Burgess—No.

CHAIR—In fact, you would be supporting that?

Mr Burgess—Totally. That is our concern. We do not want to do anything that will affect the proper use of this bill with respect to issues of clearly attacking criminality, serious police corruption—those sorts of issues. That is not what we are about.

CHAIR—You are supporting the bill but subject to these concerns?

Mr Burgess—We are concerned that a small group of police officers—and there may be potentially some others—could be swept up in this over minor disciplinary matters. For example, under the Commonwealth public sector act I do not think there are pecuniary penalties. This is unique to a few small groups of employees, one being police.

CHAIR—How do you read the Attorney-General's response in the second last paragraph, where he says that this definition therefore excludes low-level purely internal administrative or managerial actions?

Mr Burgess—I do not know that it does. That is our concern. We potentially have some sort of disagreement with the Attorney-General's letter, if that makes sense. We are not convinced that that is exactly what will be the case. As I said to Senator Parry earlier on, I have no doubt that somewhere down the line this will be tested. If we were found to be wrong, that would be pleasing.

CHAIR—He does go on to state:

… it should be emphasised that the information to be disclosed in relation to the police disciplinary proceeding must first have been obtained for the purposes of investigating a 'serious offence' sufficient to justify the issuance of a telecommunications interception warrant …

Mr Burgess—That is right. But it may have been a serious offence committed by somebody else.

CHAIR—Generally, with respect to your overview of the legislation, what operational benefits do you see for police under the current arrangements and under this new legislation?

Mr Burgess—There are many. Telecommunications intercepts and other uses of the data are an invaluable tool. We had these discussions in this room several weeks ago at the Australian Crime Commission hearings. Any tools that assist police officers and other law enforcement agencies in investigating serious criminality and corruption will be supported by us.

CHAIR—Some of the submissions that we have received draw a distinction between the definition of 'data' and the definition of 'content'. Do you have a similar view, that there is clearly a difference in definition and that they should be seen as such?

Mr Burgess—Senator Ludwig raised the definitions. I worked off what the explanatory memorandum considered to be the differences, and I was reasonably comfortable with that.

CHAIR—That is what I am checking. Are you comfortable with the proposals in terms of the definitions?

Mr Burgess—I am, albeit I have no other instructions to be other than that.

Senator PARRY—Mr Burgess, you indicated that there were two jurisdictions in the Commonwealth that do not have pecuniary penalties. Was that Tasmania and South Australia?

Mr Burgess—No. My understanding is that it is the Australian Federal Police and the New South Wales police. Although there has been some argument in New South Wales that they were silent in terms of one particular aspect, it relates to the more serious disciplinary matters. My understanding of the others, including Tasmania, is that there are provisions for fines at any level.

Senator PARRY—That is what I thought. We have received two submissions, one from the South Australia Police, signed by Commissioner Hyde, and the other from the Tasmania Police, signed by Assistant Commissioner Tilyard, indicating that both jurisdictions are comfortable with the legislation. There is no mention of secondary disclosure. Whether that is not an issue with them or whether they are expecting that it will be raised with you, I just wanted to draw that out to make sure—

Mr Burgess—It is an issue that we have focused on because it is an issue that is raised by our members. Perhaps it is not an issue that is glaringly confronting a police commissioner, who is probably more concerned about the operational aspects of a bill such as this.

Senator PARRY—I thought I would mention that they were very comfortable with that.

CHAIR—I note that today we received a submission from the Western Australia Police. Senator Ludwig has one final question.

Senator LUDWIG—I want to test your comfort with the legislation. You stated that you have gleaned from the EM what 'telecommunications data' is, and I think you gleaned that from an outline of the division?

Mr Burgess—It is on page 6 of the EM.

Senator LUDWIG—Page 6 then states:

Telecommunications data specifically excludes the content or substance of the communication.

It talks about telephone information, the parties involved, the time of the calls and the duration, websites visited and starting times of sessions. That is what you generally understand from the EM. The chair gave an example from page 13:

... for example, if during the course of the investigation in relation to taxation fraud the Australian Taxation Office obtains telecommunications data that concerns drug trafficking ...

We will dwell on that for a moment to test your comfort. It stretches my imagination how the ATO would be aware that it concerned drug trafficking if it only had available telecommunications data, as I outlined earlier, and if it did not include substance or content?

Mr Burgess—I would be drawing the link between telephone intercept and the ultimate data that was collected as a result of that. That is the way I would be drawing the link. If you take that as the example in the ATO—

Senator LUDWIG—Come back to page 13. It stated 'the Australian Taxation Office obtains'. So the ATO is able to have telecommunications data that concerns drug trafficking. How would it know that, unless, say, the IP address had 'I'm a drug trafficker' attached to it?

Mr Burgess—I would imagine that it would have been verified by other means. To my way of thinking when you look at those two, there would have been a telephone intercept. It would have clearly identified certain activities taking place and subsequent data taken, which would have included telephone numbers, and a whole range of potential contacts would have been the link between the data and the drug trafficking.

CHAIR—For example, if it went to a known drug trafficker, they know the phone number and it has been confirmed in the data that is received?

Senator LUDWIG—Does the ATO keep a list of drug traffickers?

Mr Burgess—I do not know. That would have been verified in some other way. That would have been potentially a telephone intercept and then the subsequent data collected would have supported the telephone links.

Senator LUDWIG—We will leave it to the Attorney-General's Department to provide an explanation as to how the ATO would know that—

Mr Burgess—You have put them on notice.

Senator LUDWIG—other than from the content of the material itself. What I was trying to then discover was how broad the telecommunications data is in terms of what it can actually portray. I am not really asking you to comment. The Attorney-General's Department should be able to provide a reasonable explanation. But it is a matter that can impact upon your members.

Mr Burgess—Data on its own will not always give you much information. Oftentimes the data might be verified by something else.

Senator LUDWIG—The content line or the information within it usually will provide the information. The data itself may not necessarily do that. It depends on what you include in 'telecommunications data'. It is a long piece of string.

Mr Burgess—We are concerned about minor police disciplinary offences. There is a difference if it is potential serious criminality.

Senator LUDWIG—That is accepted. Also, the law enforcement agencies have been expanded in the introduction to this legislation to include CrimTrac and others by regulation. Are you comfortable with that?

Mr Burgess—That is not an issue that we dealt with or discussed with respect to our submissions. Primarily, we were focused on one aspect. It would only be my view of the issue if I was to relay it to the committee.

Senator LUDWIG—If you do have a view about that, would you like to provide that to the committee before it reports?

Mr Burgess—Yes.

CHAIR—I wanted some clarity of the definition of an 'authorised officer'. Do you have any concerns about that definition and whether there is sufficient clarity such that you know who that authorised officer is within the management structure? Is that an issue for you?

Mr Burgess—It is not an issue that we picked up. By and large, we are supportive of the bill. None of those other issues were matters raised by our respective membership. The only issue raised was that in respect of the secondary disclosure provisions.

CHAIR—Have you sought views and comments from your members around the country?

Mr Burgess—Yes.

CHAIR—Thank you very much. I appreciate your input.

Mr Burgess—Thank you.

[2.36 pm]

GRAHAM, Ms Irene Joy, Board Representative, Electronic Frontiers Australia Inc.

CHAIR—Electronic Frontiers Australia has lodged submission No. 6 with the committee. Do you wish to make any amendments or alterations to that submission?

Ms Graham—No. There was a minor error in the original submission that we sent. We did notice that and sent a revised copy. It is my understanding from the secretariat that the copy the committee received was the amended version, so there are no changes.

CHAIR—Before I ask you to make a short opening statement, can I seek clarification as to whether you are also representing the Australian Privacy Foundation today, which has made submission No. 17.

Ms Graham—Not as far as I am aware. I was originally asked by the secretariat, if the committee wanted APF to appear and if they were not available, whether I may be willing to attempt to assist the committee with regard to its concerns. I said yes at the time but I was never subsequently advised that the Australian Privacy Foundation was being invited to appear. As far as I am aware, I am representing only Electronic Frontiers Australia.

CHAIR—I invite you to make an opening statement, at the conclusion of which we will invite members of the committee to ask questions.

Ms Graham—As you have just mentioned, we have lodged a submission, which is quite lengthy, and I do not intend to go to every point in that submission. I would like to outline our principle concerns about the bill. Our main concern is that the bill introduces significant new powers for criminal law enforcement in security agencies and civil penalty agencies. In our view, the way the bill is currently written it is not providing an appropriate balance between protecting the privacy of telecommunications users and meeting the legitimate needs for access by security and law enforcement authorities. We feel that a combination of the lack of clarity of the definition of 'telecommunications data' along with the proposed powers to access prospective telecommunication data in near real time, without a warrant or any kind of independent oversight, is a significant further incursion and interference into the privacy of individuals, many of whom will not be suspects or persons of interest because of the nature of telecommunications information that is collected from these organisations. Many of the people are merely people who have been in contact with a suspect.

Similar to the stored communications legislation last year, we are very concerned that this bill will enable tracking of people via mobile phone location information without a warrant, which is basically further extending the definition of 'telecommunications data'. It may have been considered to be that before, but I do not think the public or the parliament would have ever been aware of that. We have noted in our submission that the surveillance device legislation contains a lot more controls and safeguards over police access to tracking device use. This bill appears to have the specific purpose of allowing law enforcement agencies to use a person's own tracking device that they carry with them all of the time. Because it is a device that can be used to track a person without the need to covertly install a tracking device on a person's property or body, we believe that there is considerably more potential for misuse

of these new powers. We are strongly of the view that for that kind of information to be collected in near real time, because it will enable physical visual of track people, a warrant should be required similar to the existing surveillance device warrants in the Commonwealth and the various states, or with similar conditions attached as the stored communications warrants.

We also have significant concerns about the telecommunications data in the form of web browsing session information or internet sessions. As we have said, the explanatory memorandum on page 6 and page 8 of the bill seems to contradict itself in terms of whether web browsing information is or is not going to be defined or captured in this 'telecommunications data' definition. It is our suspicion that that is the intention of the government but, as I have said, it is certainly not clear in the explanatory memorandum. On the assumption that it is intended to be telecommunications data, we have major concerns about that, because it is not really just data. The sorts of details that they would be obtaining, being website addresses and web page addresses, are of themselves often content. Similarly, once the website address has been obtained, one can readily access the actual content that was communicated either on the website or through internet archives. Firstly, from our perspective, we feel there is a problem with this proposal to allow prospective access to web browsing information, because it is allowing access to content of communications without a warrant. Secondly, the explanatory memorandum is not clear.

Thirdly, another major concern we have concerns the reduction in restrictions on secondary and subsequent disclosure. There is a very broad extension there that will enable this sort of information that is collected to be distributed much more widely to different types of agencies and for different types of purposes than under the current law. Fourthly, as we have mentioned in considerable detail in the submission, we cannot see how internet service providers can provide prospective information in relation to email messages in near real time without engaging in unlawful interception, because there are no exceptions in the act that allow accessing and copying parts of an email message in order to give effect to an authorisation that is proposed in this bill.

We also think there are some questions about waiting until messages have been received in a person's mailbox and then accessing the mailbox to copy parts of it. We suspect that that would be unlawful access to stored communications as well. We think there are some problems with the actual drafting of the bill in terms of the technical and legislative practicality of the legislation as written. We are very hopeful that this committee's inquiry will ascertain how it is envisaged that ISPs will be able to do this without breaching the existing law.

Finally, we are very concerned with the extension of the powers to CrimTrac, which would give CrimTrac the ability to obtain stored communications warrants. We see no reason why CrimTrac should be able to get stored communications warrants because, as far as we are aware, it is not a criminal law enforcement agency or any other sort of agency that conducts investigations. It is a mystery to us why it should be empowered to gain stored communications warrants as well as the telecommunications data authorisations that are in this bill. We believe CrimTrac should be completely deleted from this legislation.

In summary, we do not believe this bill can be amended while it is being passed through parliament, because it is very complex legislation. The existing act, the Telecommunications (Interception) Act, and the other act, the Telecommunications Act, are both highly complex. Last year, the stored communications bill was amended in the parliament by the government, and we believe that led to a further lack of clarity and certainty. We are very concerned that, if this bill is amended in bits and pieces as it is going through parliament, it is likely to introduce further uncertainty and lack of clarity. We would like to see this bill put on hold until the Attorney-General's Department and the government redrafts the whole thing to resolve all the problems with it.

Senator PARRY—I take on board your remarks about the technical issues. Apart from the technical issues, the main thrust seems to be that you think CrimTrac will be given access to warrants it does not need to have access to because it is not a law enforcement agency. Is that your primary objection, leaving aside the technical issues?

Ms Graham—To the bill as a whole?

Senator PARRY—Yes.

Ms Graham—No. Certainly CrimTrac is not the major concern. The major concern is the new powers to access prospective data in near real time. We believe that should require a warrant, because it is basically interception and surveillance powers. It is completely unlike the current situation, where enforcement agencies can go to telecommunications service providers and obtain telecommunications data that the company already holds. In other words, what is available to collect depends on the operational system of the telecommunications carrier or the ISP—what they have at the time a current section 282 certificate is issued. What this is doing is asking carriers and internet service providers to proactively monitor their customers and intentionally store every piece of information they are able to store. This is surveillance and interception.

Senator PARRY—That is how I thought you started and then you married into that your opening remarks about the technical correctness of accessing stored data—how you thought that might be technically incorrect and not marrying in with other legislation. That is where I thought you were drawing the technical distinction, rather than the thrust of the legislation. So it is the thrust of the legislation you have issues with?

Ms Graham—Yes, it is the thrust of the legislation. The technical issue is a drafting issue with the bill. We are not saying that is a show stopper for the bill itself. We are saying there is a flaw in the bill that needs to be fixed if it is going ahead, but we do not think the prospective data part should go ahead at all.

Senator PARRY—Do you weigh up, in deciding as an organisation that you have an objection to the bill, the needs for law enforcement agencies to have real-time interception?

Ms Graham—We recognise that law enforcement agencies have legitimate needs to be able to access information about people's communications. Our concern with this bill is that it does not balance those needs with the privacy of individuals adequately. We believe that, for prospective information like this, a warrant similar to a stored communications warrant or a surveillance device warrant should be required. Principally, our objection is enabling just an authorised officer to authorise it, which from the explanatory memorandum of the bill could

basically be a lower manager of any of the state and territory police forces. They are able to just authorise it. They do not have to have any reason; they do not have to account for why.

Senator PARRY—But that power has to be delegated down from a commissioner of police or a head of agency; it is not an automatic right.

Ms Graham—Yes, but it is still just an officer in an enforcement agency making a decision that they want the information. It is quite different from the conditions attached to getting a stored communications warrant, where the magistrate has to take into account various considerations and so forth. We do not feel that an agency officer is capable of appropriately weighing the balance in any particular instance. That is why we think there should be independent oversight in determining whether access can be granted.

Senator PARRY—In relation to CrimTrac, and item (m) on page 5 of your submission, I am not really sure why you are concerned with CrimTrac. Could you outline again your major concern with CrimTrac having the historical telecommunications data? Is it that you do not want them to store it, full stop—or anyone to store it?

Ms Graham—From our perspective, the issue is about CrimTrac, because in relation to definitions of the enforcement agencies it is being added to the existing definition. As far as we know, it does not have any investigatory powers. We simply cannot understand why it would need to get a warrant to access stored communications or issue authorisations to access telecommunications data. Basically, we want to know what CrimTrac would be going to do with it. As I have said, our understanding is that it is not empowered to investigate crimes. This is my speculation as to the reason for putting CrimTrac in there. It is my understanding that CrimTrac maintains a number of databases. I do not know exactly what is in them other than what it says is in them in its reports to the privacy commissioner each year on the types of databases it holds. That information tends to imply that in the databases it holds the information is mainly about people who have been charged at some stage. The combination of adding CrimTrac into the definition of enforcement agencies, together with removing the restrictions on secondary and subsequent disclosure, appears to be setting up a situation where every piece of telecommunications data collected by any criminal, civil or pecuniary penalty or public revenue agency that obtains telecommunications data can be shot off to CrimTrac, which can build a massive database about everybody who has ever been communicating with someone who is a person of interest or who is a person of interest. Maybe that is not why CrimTrac is being added in, but that is what this bill does. It enables all agencies to send every piece of information, whether or not the person has ever been charged, to CrimTrac to put into a database. That is a concern. We want to know what CrimTrac needs this information for, since it is not empowered to investigate of its own accord.

Senator KIRK—Can you elaborate on the assisted GPS technology—the growth of the technology, the way it will have an impact and how it is relevant to the terms of this bill? Not being someone who has a great deal of understanding of the technology, I wonder whether you can explain it for us.

Ms Graham—Unfortunately I am not going to be able to help you a lot, because I looked into that aspect only very recently and merely read some information that was brief about

assisted GPS. I am not purporting to be a technical expert on assisted GPS, because I have not looked into it to any depth, but my understanding is that at the moment the mobile phone locational data is purely being worked out via triangulating between mobile phone towers in various places to estimate that a mobile phone is in the middle of three locations. However, assisted GPS effectively turns a mobile phone into a tracking system, the same as GPS systems in a car; the accuracy will become vastly better. There have been media reports over the last couple of months speculating that Telstra is intending to introduce assisted GPS on its new G3 mobile network in 2007 or 2008. I am not saying it definitely will; I am just saying that the pundits are speculating that that is on Telstra's agenda. Whether it is on Telstra's agenda or not, assisted GPS exists. It is just a case of which carrier introduces it first as to how quickly we see this narrowing down.

Senator KIRK—Are you saying that currently there can be an estimation of where the phone is from the way the towers are set up?

Ms Graham—Yes. There are a few companies that are providing that service at the moment in Australia. My understanding is that it is mostly used for businesses such as trucking companies, which have started giving drivers mobile phones so they can track trucks with mobile phones and can know when they are due at the next place. The businesses using Telstra and other carrier provided data claim on their website that their accuracy at the moment without assisted GPS is within 200 metres. One that I came across claimed that in some urban areas it can be accurate to within 100 metres. My understanding is that is a radius of 200 metres. As I have said, assisted GPS will reduce that to within a 100- or 200-metre radius, and that is a concern—that is pretty accurate.

Senator KIRK—Your concern is that this prospective information is already accessible and its use will increase.

Ms Graham—Yes. My understanding is that at the moment there is nothing in the existing law that says agencies can go to a telecommunications carrier and get prospective mobile phone location data in near real time. At the moment they would have to put in a request and they would get everything that the carrier had up to that point in time. Of course, whether the carrier would have any information about where the mobile phone had been would depend on whether they were in the habit of checking that and keeping records of all their customers. I suspect the probability of that is near zero, because I cannot imagine why Telstra, Optus or Vodafone would be regularly checking where each of their customers' mobile phones were. I doubt very much at the moment whether enforcement agencies have been getting any mobile phone location information for that principal reason; I just do not think it would have been available, because the section 282 certificates that can be issued at the moment apply only to data that exists up to the point that the authorisation is received by the carrier. This would change that and it would now be telling the carrier they had to have a means of in near real-time, for the next 45 or 90 days, of locating where a particular customer is. To EFA that is clearly a surveillance and tracking system. It is really not about telecommunications data; it is simply using the person's mobile phone as a tracking device.

Senator KIRK—I also want to ask you about section 280. You suggest that there ought to be an amendment to section 280 of the Telecommunications Act. Can you elaborate on that? You mentioned that this committee made a recommendation last year about that.

Ms Graham—This was an issue raised in the hearings last year and possibly even in the previous TI amendment bill hearings. The core of the issue is that section 280 of the Telecommunications Act states that in effect carriers, ISPs and so forth can disclose information or a document to an enforcement agency if it is done under a warrant—and that has been in the act since 1997 or even before that. When the stored communications warrants came into effect via amended legislation last year, the government said initially at least that the intention was that, after the bill was passed, the sole means of access by law enforcement to the content of stored communications would be through a stored communications warrant or an interception warrant. Our view is that the Telecommunications Act section 280 leaves that open to question because it says 'under a warrant'. It does not say 'under a warrant under the Telecommunications (Interception) Act'. Our concern remains that that appears to be suggesting that, for example, state and territory agencies, be they criminal or other types of enforcement agencies, can potentially come along with a general search warrant and not a stored communications warrant. Can they get the content of stored communications with a general search warrant? Section 280 of the Telecommunications Act appears to say they can, and yet anybody who has read the explanatory memorandums of the TI bill last year would be under the impression that they need a stored communications warrant.

The problem is being worsened by this bill, which is part of the reason that we have raised it again, because the Telecommunications Act is also being amended in section 313, the section that discusses what carriers have to do to provide reasonably necessary cooperation or help to law enforcement authorities. This is adding a new clause that is specifically referring to section 280. That clause in the existing Telecommunications Act never referred to section 280. The fact that it is now being added in seems to further confirm that in fact they do not need a stored communications warrant to get access to content.

Senator KIRK—It is a matter of getting some clarification.

Ms Graham—It is because section 280 refers in specific to an enforcement agency. It is not talking about court issued subpoenas or notices to produce by the court in family law court matters. It is not talking about anything else. The very first item in section 280 is specifically referring to enforcement agencies. Our issue is that content should not be accessible without a stored communications warrant, and section 280 of the Telecommunications Act is muddying the waters. It needs clarity. It either needs to be deleted or it needs to say that this does not include content or substance of communications.

Senator KIRK—The way that you have described it, without a stored communications warrant, which specifies it was that type of warrant?

Ms Graham—Yes, or an interception warrant.

CHAIR—Thank you for your submission. Going back a step, did you have input into the Anthony Blunn report and recommendations?

Ms Graham—Yes. We lodged a comprehensive submission. We made recommendations, many of which were substantially similar to what Mr Blunn ended up recommending and what was in the bill last year. We were generally in support of the stored communications bill last year. We had some issues with parts of it, but its overall principle was very similar to what we had recommended in our submission to the Blunn review.

CHAIR—In the main you supported the Blunn report and recommendations and then you supported in the main the bill of last year.

Ms Graham—Yes, that is right. We were happy with the basic policy decision that the stored communications warrant would be required. To the extent that we had any disagreements, they were around the detail of the wording and that kind of thing. We were happy with the policy position of that bill last year, which reflected what was in the Blunn report—namely, that the content and substance of telecommunications information should not be accessible without a stored communications warrant.

CHAIR—Thank you for that. You have made some pretty strong observations and recommendations today with regard to the over-reaching nature of the bill before us—I think that is how you would describe your perspective—and the blurring of the definition of 'content' and 'data.' You have used the example where people go to a website to access this, that and the other, I notice it is a date of a public meeting as per your submission. I have been looking through the list of submissions that we have received but we have only had one from an ISP or an ISP that is part of a group, so what is your thinking behind this being a significant issue for ISPs? How would you rationalise that? If it is such a concern, why are they not represented at the table or in the submissions to the committee?

Ms Graham—I would say that is a very good question. EFA has been submitting to this particular committee on telecommunications interception laws since the first of the changes to email and so forth laws. It is my recollection that in that entire time there have been very few submissions to the committee by any members of the industry. It is my view that that is principally because carriers consider it their responsibility to comply with the law; if the law says that they have to do X, Y and Z then they will just do it. None of them really want to upset government because they are worried about getting even more regulation over their activities than already exists. Generally speaking, they only submit when it is a matter that is going to interfere with their ability to compete in the marketplace and things like that. On general matters where it concerns the privacy of their customers and that kind of thing basically they do not submit to parliament.

CHAIR—You are saying to us today in your submission that it is going to have an impact on the way that they do their business and the way that they operate.

Ms Graham—I do not know whether it will. It is unfortunately exceedingly likely that many of the ISPs, especially the smaller ones, have not looked at the detail of the bill to be aware of its impact. I presume you are talking about what we are saying about the technical ability to do what is required without engaging in unlawful interception. For any carrier or ISP to submit to any of these inquiries, they need to be first of all aware that the bill even exists. Secondly, they have to read the bill and go back to the previous legislation and identify all of the little definitions that were put in last year and all of the minute changes to even notice the kind of thing that we have raised in our submission. To be quite honest with you, I do not think that there is that level of interest in industry about the detail of legislation. Most of the industry would take the view: 'This law says that we have to provide reasonably necessary help to the police. So if the police come along and say we want this, we must be allowed to give it to them.' I would really query how many of them actually read the detailed law.

CHAIR—That is a fair question from the committee's behalf—

Ms Graham—Yes, I agree. I have pondered at length myself why the industry does not submit.

CHAIR—You would think that the Internet Industry Association would be an industry representative body.

Ms Graham—Yes, you would think so.

CHAIR—I am sorry I am not more up to date, but could you just advise me as to who you represent exactly?

Ms Graham—Electronic Frontiers Australia.

CHAIR—Yes.

Ms Graham—Do you mean who is Electronic Frontiers Australia?

CHAIR—Yes.

Ms Graham—We are a non-profit membership based organisation Australia wide. We represent individuals who are internet users and telecommunications users. Principally our objective is aiming to protect rights and freedoms in use of the internet. We are specifically concerned with individual's rights and freedoms. We do not represent any industry or enforcement-related bodies. We are purely a membership based organisation representing ordinary individuals.

CHAIR—There is a summary in part about EFA at the back of your submission. You have put in a very substantial submission. I appreciate that and thank you for your input.

Senator PARRY—I just have one comment. I could not let Ms Graham go with the comment that the ISP people would be under the threat that we will give them more legislation if they do not cooperate. I just wanted to make quite clear that we do not govern that way.

Ms Graham—I was not intending to suggest that you did. It is that I have heard that kind of comment behind the scenes from people in industry. It is the 'don't rock the boat' scenario. I was not meaning to imply that there was any threat.

Senator PARRY—As long as that is recorded as not an accurate comment.

Ms Graham—I am sorry.

CHAIR—Thank you Ms Graham for your evidence today.

[3.10 pm]

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

RYAN, Mr Michael, Member, Australian Mobile Telecommunications Association

CHAIR—I welcome witnesses from the Australian Mobile Telecommunications Association and Telstra.

Mr Ryan—I should make clear that although I am a regulatory manager, future network and services, Telstra, I appear as an AMTA member.

CHAIR—AMTA has lodged submission No. 5 and Telstra has lodged submission No. 9. We thank you for that. Do you wish to make any alterations or amendments to your submission?

Mr Althaus—No.

CHAIR—I invite you to make a short opening statement, after which we will have some questions.

Mr Althaus—Thank you for the opportunity. The Australian Mobile Telecommunications Association is in fact the peak body for the mobile industry. The members of AMTA include carriers, handset manufacturers, infrastructure network vendors and various other suppliers to the industry, even down into the retail chain. We have, of course, been part of the debate for some time now surrounding this and other pieces of legislation in the government's agenda in the law enforcement national security arena.

AMTA generally supports the TIA bill, as we have come to refer to it, and recognises that the assistance that the industry can give to law enforcement and security agencies is a key and important part of national security objectives. To that extent we are broadly supportive of the package and this particular bill. We also recognise that there are changes. We are in a very rapidly moving sector, so both technologically and structurally there is frequent change. To the extent that legislation needs to cope with that change, we recognise the ongoing need for adjustments from time to time. Indeed we are, not surprisingly, strong proponents of the elements of the Telecommunications Act, particularly those that refer to self-regulation and of course the imposition of regulations such that not undue financial or administrative burden is placed upon the industry. We also recognise that, through the co-regulatory path that we often have the opportunity to take, we get a built-in flexibility in solutions that industry can bring to bear and, in a partnership with government, we can reduce the need for black-letter law so that the industry can go about its business again with flexibility and an ability to respond to changes in technology.

Against that background, we are concerned with the balance, particularly between law enforcement, national security issues and the world in which telcos operate and of course we are and do seek to remain competitive in the market, particularly given the global nature of the information flows these days. Of course stakeholder expectations of returns are key to our thinking as well, and maintaining competitiveness of the individual enterprises. That is part of the balancing act for this industry because fundamentally—I will say it again—we recognise,

respect and are willing participants with government on issues relating to law enforcement and national security insofar as we can be part of solutions in that regard.

Having said all of that, there are elements of the current bill which we have raised in our submission. I would have to say most of them appear to be relatively administrative and operational fine-tuning, if you like, rather than any fundamental concerns. I would emphasise to the committee that the industry's level of consultation on this bill has been reasonable but variable. Frequently time lines have been a challenge. We look at the current state of the bill and note that some of the consultation process that was explicitly within the bill is no longer there. The extent that that changes the attitude of government in terms of consultation remains to be seen. We do not believe that it will but we note the omission of some of that formal consultation that was in an earlier draft.

We would like to turn to the operational points now in terms of the fine-tuning of the bill that relates to the industry. I will give you a first example and then my colleague can give a couple of others. These are the main issues raised in our submission. We are particularly keen that those elements of the Telecommunications Act that I referred to earlier are reflected in the bill and the bill does do that specifically. The Communications Access Coordinator role seems to be one that is particularly pivotal and we would like to see the objectives of the Telecommunications Act picked up by the CAC, as we are going to call him or her. Regrettably, I am sure it is an acronym that will stick. The CAC's having due regard to the objects and policy objectives of the Telecommunications Act is something that we would like to see recognised and being a formal part of this bill. I will pass to Mr Ryan, who will make some further comment.

Mr Ryan—Under section 187, which deals with definitions, we believe that basically the intercepting capabilities have been slightly redefined in that the bill has broadened that definition to include things like mobile handsets. Currently, the interception capability obligations on a carrier are on what we control—in other words, the end-to-end network. We believe, under the redefinition in the amendment bill, that has been broadened to include things like handsets, which we have no control over, and also applications that may be hosted overseas such as Skype or Yahoo et cetera. We are concerned that the definition of 'interception' has been extended to handsets, CPE, that we do not control—they are under the control of the customers—and also applications that may be hosted from overseas. We can undertake interception on our own networks; that is not a problem. We have to do that and we comply with it. But when it comes to networks that we do not control or customer equipment that we do not control, it is certainly outside the realms of the carrier being able to undertake that activity.

Under 'delivery point', Telstra has a delivery point in Melbourne. The problem with section 188 is that the delivery point could be specified as Perth or Sydney or somewhere like that, so it makes it very difficult for those carriers, or CSPs, being told to deliver any intercepted material in a physical location other than where their delivery equipment is. It is very specialised equipment.

Section 192 deals with the ability of the CAC to grant exemptions. We are not saying that you cannot grant exemptions and that you cannot have that ability, but from our point of view the CAC has 60 days to consider an exemption application, and it is deemed after 60 days that

you have got an exemption. The problem is that CAC can come back and say you no longer have that exemption, which then leaves us in a state of uncertainty as to what we do with those applications. Where the period goes to greater than the 180 days after the lodgement of that exemption application, we are asking that the agencies have to demonstrate that there is a need for interception of that particular product or service. At the moment we have an exemption application that has been granted for a health video link for a number of hospitals in Victoria and we do not know how long that exemption will actually go for. It makes it very uncertain in terms of delivering advanced services to customers if there is no time line or dead end to the deemed period.

Mr Althaus—The nature of an interception capability plan is dealt with in section 195. In the view of the membership that has brought together this submission we are looking at an expansion of the factors that need to be included in that plan. That goes to an inclusion of a change in marketing or pricing of services. Again, it is an operational thing, but this is the dynamic nature of this industry. That sort of change would take place relatively often so we would be comfortable with the notion of this applying to significant technology changes, but in a day-to-day sense there is technology shift of a minor nature and certainly, in terms of the marketing and pricing of services, that could present quite an onerous burden on industry to be responding to that.

Finally, again going to our views around the CAC position or indeed ACMA and again in relation to interception capability plans, we are looking at a reasonableness test. There does not seem to be any specific definition of how the CAC or ACMA would test reasonableness, so some extra definition there would be helpful.

CHAIR—Thank you for that evidence. Senator Kirk?

Senator KIRK—I will go back to section 6R and the addition that you are proposing there. You have said that the CAC ought to take into account the objects and regulatory policy of the Telecommunications Act. I am wondering what that really adds. Is it the case that one would have thought that the CAC would take those into account? So what is really being added by that?

Mr Althaus—We are looking for an explicit reference to those elements of the Telecommunications Act and the CAC position. The CAC position is going to be a very powerful and pivotal role in the operation of this bill. One of the key tenets of our discussions with government over time on this has been some of those fundamentals of the Telecommunications Act that we wanted to see reflected in this bill. This, to us, is a tightening of that.

CHAIR—What further does it add to the current bill as it is drafted? Would you be anticipating that they have to take into account the objects of the act in any event?

Mr Althaus—It would. Again, it is simply a belts and braces approach, from our point of view, in relation to the CAC.

CHAIR—It is just tightening it up even further?

Mr Althaus—Yes.

Mr Ryan—From our point of view, under the Telecommunications Act it basically promotes greater practical use of industry self-regulation. Basically we are asking that we are considered or be involved in discussions around proposed legislative changes. We are looking for input that allows us to implement the practical side of the legislation.

Senator KIRK—With respect to section 187(2), I heard what you said in relation to it extending to matters over which carriers have control. You mentioned that you have no control over handsets and overseas applications. I wonder whether it should be the way you have suggested with the two subsections (d) and (e), where you actually specify customer equipment and then that is applying a content service, or whether it would be better if there were to be a reference to matters over which the carrier has control or does not have control.

Mr Ryan—Yes.

Senator KIRK—Would that achieve the same thing as you are suggesting?

Mr Ryan—Yes.

Mr Althaus—The operational reality is what we are trying to get to here. There is a changing landscape and a great number of areas where the carriers do not have the influence.

Senator KIRK—That is what I was thinking if you specify two matters and then if things develop further.

Mr Althaus—Yes.

Senator KIRK—I would like to go to clauses 198(3) and (7), being the interception capability plans. In many ways this is perhaps similar to the first question that I asked. I wonder what it adds to say that the objects and regulatory policy of the Telecommunications Act should form part of the reasonableness test? Is that similar to the point that you were making in the first instance in relation to the CAC?

Mr Ryan—Yes.

Senator KIRK—It is really just for clarity rather than anything else?

Mr Ryan—Yes.

Senator PARRY—I refer to clause 188 in the bill, which deals with the delivery point. Mr Ryan, you made reference to the fact that one location of yours is Melbourne. I did not quite understand the technical difficulty that you would have with this particular definition of this particular delivery point?

Mr Ryan—If we have our specialised equipment in Melbourne then we would like to deliver in Melbourne.

Senator PARRY—That is not stopping you doing that, is it?

Mr Ryan—No.

Senator PARRY—I did not understand the issue. You had a concern that you did not feel as though you could technically comply with 188?

Mr Ryan—It is basically currently open to interpretation, if you like. It does not matter which carrier it is: we would like to deliver in the same locality as we have got our delivery equipment.

Senator PARRY—So what you are saying is you would like multiple locations to be able to do the delivery point?

Mr Ryan—If there was another carrier in Sydney, I would like to deliver in Sydney, because that is where my delivery capability would be.

Senator PARRY—How does that affect you operationally? What is the operational issue? I gather that the Communications Access Coordinator can access the information from one location rather than dozens.

Mr Ryan—It may not have a big impact on a large organisation which has a presence in many centres, but it will have on a smaller ISP who is located only in Perth.

Mr Althaus—The other issue is the consideration of the relationship between the delivery capability obligation and where the delivery points are. Again, it is getting to that sort of operational practicality side of things in terms of capability versus delivery point.

Senator PARRY—In relation to having a reasonable charge, part of your submission was that you wanted to be reasonably compensated—not making a profit and not making a loss—for providing this information.

Mr Ryan—Yes.

Senator PARRY—Would there be a common fee or charge that you think could be applied across the entire industry?

Mr Ryan—At the present time the charges differ between different carriers or CSPs. It is based on the cost to them of actually undertaking the activity. As to a common fee, it can make it very onerous on, say, a smaller ISP, whereas on a large one they may not see the difference. Again, it just depends on the ISP or the carrier's capabilities and what resources they have currently employed to meet that interception and delivery capability.

Senator PARRY—Do you think that the amendments to the legislation will enable the legislation to keep up with emerging technology? Can you see that we will have to come back here in another six months time and amend again or do you think we are catering for as much as we can possibly foresee into the future?

Mr Ryan—I think the legislation is catering for as far as it can see. It tries to be technology neutral, and we see the same legislation around the Telecommunications Act. They are the same objectives there but everybody in the industry is struggling in some way or other in trying to look far enough into the future to determine, not so much from your side of things but from our side of things, as to how we comply with the legislation. There are a number of issues coming up for us that we have got to take a lot of time and effort to sort out.

Senator PARRY—Do you speak with comparable organisations and industry associations internationally? If you do, do they have better or worse legislation models or how do they comply with telephone interception issues?

Mr Althaus—It is highly variable. In answer to the first part of your question, yes, we do measure ourselves against what other industry sectors around the world are doing. Australia is well positioned in the mobile space, particularly. We do not feel through our comparative work that we are particularly facing a more onerous obligation, but nor are we lagging behind.

One of the challenges for government in this particular context is how to deal with the rapid change in technology and the frequency of that change. Of course in this context the expanded use of telephony services and now their combination with data services—the convergence of internet with telephony et cetera—and future proofing and getting a legislative construct that is going to survive in the long term is one of the challenges that Anthony Blunn faced. In many respects it is just a matter of drawing a line and making that clear and operationally viable for industry. We do not for one minute think that this issue is closed.

CHAIR—I would like to go back to Anthony Blunn. You had input into the Blunn report and recommendations. Were you supportive in general of the recommendations?

Mr Althaus—We did have input and generally, yes. I just want to reiterate the industry's attitude to this whole sphere of operation and cooperation with government. Like any legislative package, there were barnacles that we sought to knock off along the way but for the most part we were reasonably comfortable with both the process and the outcome.

CHAIR—In terms of the process and the outcome of this exposure draft bill, there has been consultation with your industry. You touched on that in your introductory comments. Were you satisfied with that consultation and did you feel as though the views that you put were perhaps in part taken on board or that some were not taken on board? Can you give us an overview because I noted that you specifically said that there was an omission of consultation in the bill. That is my next question. I would like you to specifically address that for the committee if you possibly could.

Mr Althaus—There was over an extended period a high degree of interaction with the industry. We had a number of concerns particularly in relation to standards and powers within the exposure draft. We were able to put an argument forward, the government listened to that, and that was an important amendment in our view. In many respects it was the most important amendment that came forward. You find that we are somewhat obsessed about the relationship between this bill and the Telecommunications Act and the acknowledgement of the objects. In the exposure draft there was a consultation process outlined explicitly and that has been removed from the bill as it currently stands. I suspect that is on the basis that the standards issue had largely been solved, but in this context we go to our point that this is a partnership between industry and government and, to the extent that there is a strong flow of discussion and negotiation between the two, that can only give a better outcome from both sides. We looked at consultation during the process and felt reasonably comfortable with that but we also looked into the future as to how consultation should be built into how the bill is managed, and that was the point of the omission.

CHAIR—Have you made a specific recommendation in that regard?

Mr Althaus—No is the answer to that question specifically. It is referred to in general terms that consultation be a feature of where industry and government interact on this bill.

CHAIR—I could not see it in your submission or the Telstra submission. I want to go to the Telstra submission where it talks about matters to be taken into account by the minister under section 189(4) and adds four dot points, with the second dot point specifically being:

- the effect of the determination on the ability of the telecommunications industry to introduce new and innovative products and services;

Senator Parry has touched on that. That is basically changing technology. And then the next dot point is:

- the effect of the determination on existing products and services in the market, including the costs to be incurred by carriers in ensuring that existing products and services in the market are compliant with the determination ...

Is it right that you believe that the current section 189(4) is inadequate and needs to be broadened to take into account new technology and any costs to the industry? Do you want to expand on that and give us the reasons why?

Mr Ryan—I would like to take that on notice.

CHAIR—All right, Mr Ryan. Do you have an indication regarding the costs to the industry of this legislation and how they may impact either on Telstra or on AMTA members?

Mr Althaus—Not at this point.

CHAIR—Are they marginal or nominal—or you have not got a view at this stage?

Mr Althaus—We have been working through the implications of the bill and how it is going to affect us operationally across the board. Again, with such a broad remit, that sort of analysis has not been finalised at all at this point in time.

CHAIR—You put forward quite a number of amendments. Would you care to prioritise them? Let us say you had three. What would be your top three priorities? I know this is a tough question, but I would appreciate if you could have a stab at it.

Mr Althaus—We typically want all.

CHAIR—Of course you do. If that is your answer I will accept it. Are there one or two that perhaps stand out from the others? If not, that is fine; I am just testing you.

Mr Althaus—Some of these are quite small operational elements. Of all of the things that we have raised, most particularly in relation to the interception capability plans and the role of the CAC, again these things operationally will probably be bedded down, but they are not necessarily our highest priorities. I guess the submission reflects issues that we have stripped down to those that we would like to see addressed.

CHAIR—Can we assume that you have had some liaison with the department during the consultation on the exposure draft on those matters and that, as a result, the department has not seen those matters in the same way that you have?

Mr Althaus—Yes, you could assume that. The way the consultation has gone has been pretty typical. There have been things raised. Each and every one of these things have been specifically discussed, and I would be reticent to say. We have certainly had an open and fruitful dialogue with the department.

Mr Ryan—From an industry perspective, since the Blunn report came out discussions and consultations particularly with the new Telecommunications and Surveillance Law Branch have certainly improved. They have certainly been open. We have got on quite well in terms of discussing issues.

Mr Althaus—One of the issues to be addressed at this point in time, one which exercises the industry's mind, is the nature of the ongoing interaction between the department and

industry. We have mentioned other bodies within the domestic industry, and AMTA is seeking to bring those bodies together and has had a discussion with the Attorney in relation to a high-level strategic forum whereby industry and the department can engage in higher level discussion in addition to, and complementary to, the operational issues that get discussed in other forums.

CHAIR—Electronic Frontiers Australia put to us some of the definitional concerns that they had about content and data and the difference between historical and prospective data. Can you relate to those concerns or do you have concerns of a similar ilk?

Mr Ryan—No, we do not. The changes as to 'prospective' do—for want of a better word—tidy up some of the issues that are currently there.

Mr Althaus—Some of the definitional stuff we just see as being worked through operationally with the department, ACMA and the CAC.

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

Proceedings suspended from 3.41 pm to 4.02 pm

CURTIS, Mr Jonathan, Director, Attorney-General's Department

KELLY, Ms Wendy, Assistant Director, Attorney-General's Department

MARKEY, Mr Lionel Wayne, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department

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

LAMMERS, Federal Agent Rudi, Acting National Manager Border, Australian Federal Police

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

CHAIR—Welcome. The Attorney-General's Department has lodged submission No. 15. I remind senators that the Senate has resolved that an officer of the department of the Commonwealth or of the state shall not be asked to give opinions on matters of policy and shall be given reasonable opportunity to refer questions asked of the officer to superior officers or to a minister. This resolution prohibits only questions asking for opinions on matters of policy and does not preclude questions asking for explanations of policies or factual questions about when and how policies have been adopted. Officers are also reminded that any claim that it would be contrary to the public interest to answer a question must be made by a minister and should be accompanied by a statement setting out the basis of the claim. I invite you to make a short opening statement, at the conclusion of which we will invite senators to ask questions.

Ms Smith—I will not repeat any matters that are already set out in our submission or in the Attorney-General's second reading speech, but instead I would like to focus on two key points in relation to the bill. The first point is that this bill brings together all provisions governing national security and law enforcement access to telecommunications into one act to create one piece of overarching legislation that governs access to communications. This implements the core recommendation of Mr Blunn in his review of regulation of access to communication. This change is intended to make the nature and scope of these access powers clearer to agencies, industry and to the public alike. It will also clarify the relationships between the three types of information, being telecommunications interception content, stored communications content and telecommunications data.

The second important point this bill addresses is that it is assisting the legislation to deal with the convergence of technology. In recent years there has been a dramatic increase in telecommunications technology and within the industry that provides it. The driving force behind these changes has been the convergence of technology and services, and the emergence of internet based services. This means that different methods of electronic communications are converging into a single extraordinarily complex data stream. A device such as a mobile phone, which until recently was a single service we could use to call someone, is now a portable office, providing multiple services such as SMS, MMS, email, video calls, file transfers, web browsing and so on. These developments have fundamentally changed the way law enforcement agencies need to conduct their investigations. It has also

dramatically increased the complexity of the relationship between agencies and the telecommunications industry. With the convergence of these technologies, it is essential that law enforcement and national security agencies retain their ability to lawfully access these services to combat serious crime and terrorism. For agencies and industries alike, the line is now blurred in what level of access is appropriate for agencies. With one overarching piece of legislation there is a greater certainly in place on how agencies can receive assistance from the telecommunications industry.

In developing this bill there has been major consultation with key stakeholders. In February an exposure draft was placed with major stakeholders. In the resulting discussions we received a lot of constructive feedback and suggestions, and many are reflected in the current bill before the committee. To assist the committee's consideration of the bill, we have put together some additional items, which I seek to table. The first is a table making a comparison between the existing provisions within the Telecommunications Act and their equivalents in the proposed legislation. The second is a diagram that addresses what would be the three types of access to communications under the new proposed bill and the current Telecommunications (Interception and Access) Act. The third is a diagram of a model of how the processes of interaction between agencies and industries works in practice.

This bill essentially is a refinement of the current administrative and legal arrangements in place under both the T(IA) Act and the Telecommunications Act, and my officers and I are more than happy to answer any questions specifically on the bill.

CHAIR—Would the Federal Police like to make an opening statement?

Federal Agent Lammers—The Australian Federal Police feels it is unnecessary to make an opening statement, other than to say that we support the statements made by the Attorney-General's Department.

CHAIR—We will move to questions.

Senator LUDWIG—You have had an opportunity to hear some of the evidence today from the Police Federation and Electronic Frontiers. Is it your intention to go through each of those submissions and provide a response to some of the matters raised?

Ms Smith—That was not our intention, but we could do that should the committee like us to provide that at a later date in writing.

Senator LUDWIG—I will deal with individual matters relating to the Police Federation first. The EM does not have a definition of 'telecommunications data' but it has an explanation of what it includes. The bill does not include a definition of what 'telecommunications data' is.

Ms Smith—That is correct.

Senator LUDWIG—Is it the intention to put a definition in?

Ms Smith—No, it is not the intention. The T(IA) Act has been technologically neutral. One of Mr Blunn's comments is that it has been very robust in the face of technological change over the years. Our concern about defining what technology and call associated data may be now might be redundant in 12 months time. Essentially we rely on the premise that the contents and substance of a communication are protected and are only accessible under a TIA

warrant, an interception warrant or a stored communication warrant, and it is the other information that attaches to a communication but does not disclose the contents or the substance of that communication that is the associated data. One of the points of bringing this all into one piece of legislation is the hope that by having the three limbs together it will be clearer when advising law enforcement and the carriers on what exactly is content and what is call associated data as new technologies come into place.

Senator LUDWIG—Mr Mark Burgess of the Police Federation of Australia took the committee to the Attorney-General's letter of 28 May, where there was concern by the Police Federation of Australia that disciplinary proceedings may be caught in various jurisdictions by the phrase a 'pecuniary penalty'. The view of the Attorney-General seems to be as stated in the letter, '... nor will they permit the general use of telecommunications data and police disciplinary proceedings …' As a consequence, do you need to amend the bill to take a belt-and-braces approach to ensure that it does exclude disciplinary procedures? We have heard some evidence that it could include fines in various state jurisdictions. If there are fines in state jurisdictions, that would amount to a pecuniary penalty and therefore it could apply.

Mr Curtis—The difficulty with these provisions is that they have to try to get across police legislation in each state and territory. What we have adopted is a general approach that sets a standard at pecuniary penalty. As Mr Burgess stated, the only matters that attract pecuniary penalty under the legislation would enable access, and that will in practice exclude a lot of the more minor or administrative offences. It is also important to note in this context that all the information that would be disclosed would in any case be available to internal investigators for those offences under the usual existing 282 provisions, and also that the information that would be disclosed for the purposes of that police disciplinary offence is material that the investigators actually have and know is relevant to a particular investigation. Our view is that, from a public policy point of view, it is appropriate that they should be able to pass on that information and disclose it when it is held.

Senator LUDWIG—In summary, the view of the Attorney-General's Department is that there is no need to change; it includes a pecuniary penalty and the protection of public revenue and that that should remain and that there is no need to change the bill?

Mr Curtis—Yes.

Senator LUDWIG—With respect to the protection of public revenue, is that a usual phrase that is found in these types of bills? Can you explain what that means?

Ms Smith—It is taken out of the current Telecommunications act, and I understand it has been there since 1997. Agencies such as the Taxation Office, the Child Support Agency and ASIC all take advantage of that particular interpretation in obtaining information to enforce their particular role.

Senator LUDWIG—Have you had an opportunity to look at the Electronic Frontiers submission?

Ms Smith—Yes, we have.

Senator LUDWIG—Is there a document that sets out a response to the Blunn report in terms of the findings and recommendations that have been made and those accepted and those rejected by the AGD?

Ms Smith—It is my understanding that, assuming those provisions are in the current bill, only two or three recommendations have not yet been implemented. A number of the recommendations by Mr Blunn were administrative in nature. But it is something that we could certainly put together in a very short space of time.

Senator LUDWIG—That would be helpful. The question really went to whether there was a government response to the Blunn report?

Ms Smith—No, there was no government response to the Blunn report.

Senator LUDWIG—Do you know whether there is an intention to provide a government response to the Blunn report?

Ms Smith—I would have to take that on notice.

Senator LUDWIG—We can then follow on to the next question, which is of course: can you provide an outline in terms of the Blunn report of those recommendations that have been implemented and those that have not been implemented?

Ms Smith—The department could provide that information to you.

Senator LUDWIG—That would be helpful. Can you comment on those that have not been implemented as to the reason they have not been implemented?

Ms Smith—No, I cannot.

Senator LUDWIG—Do the current bill and the schedules fall under the Blunn report? In other words, were all of the findings and recommendations made by him and, if not, which ones were not?

Ms Smith—No, there are one or two additional provisions.

Ms Kelly—Basically, schedule 1 of the bill falls under the recommendations of the Blunn review. It is schedule 2 that we would be looking at. Where we have provided the definition of 'child pornography' into a serious offence that is an additional amendment and is outside the Blunn report. There are also a number of technical amendments in relation to state and territory legislation, which has been changed over time and is referred to in the TIA act and that we have carried through.

Senator LUDWIG—It would be helpful if you had a table that set out those in schedule 2 that fell outside and where they came from—in other words, impetus for those amendments. It does not have to be particularly detailed.

Ms Kelly—There are probably three or four.

Ms Smith—One of the tables that we provided to you today addresses all of those provisions that have been moved over to create the overarching legislation. There are some references in the current act and in the current bill.

CHAIR—Is that the comparison of provisions table?

Ms Smith—Yes. We can do one for schedule 2 as well.

Senator LUDWIG—That would be helpful. EFA raised concerns about prospective information concerning access powers in relation to mobile phones. I am not sure I understand the technology particularly well. You might be able to help me with that. I am speaking about the ability to track mobile phones using GPS data. The Law Council also mentions in its submission that it has some concerns about that and whether or not any consideration has been given for provisions under the surveillance devices legislation laws to operate here. If they can track mobile telephones in real time or in near real time then are you effectively tracking the person? Should that then fall within the surveillance devices legislation? If that is the case, it could be dealt with there. If it is more appropriate here then shouldn't at least the provisions be consistent? That is the general tenor of the arguments being put forward.

Ms Smith—Access to prospective data already exists under the current regime. In moving it over to the TIA act, we have acknowledged that there are two accesses under section 282 of the act—that is, historical data and information in real time. It is the same information that is accessed under both regimes. It is basically that I called you—my phone number, your phone number. It is the sort of information that is on a telephone bill. If we are using our mobile phones, it will say something like I was in Barton and you were in Parkes. It is that sort of information. As to the idea that it can be used for tracking, a mobile phone sends certain signals up to a cell site indicating that we are in a certain location. At the moment the technology is not such that it will pinpoint where either of us are to any level that you could actually track a person to any point. It could not say that my phone is on at the moment and on silent, but it can say that I am in a particular geographic area. It will not say that I am at Parliament House necessarily and it will not say that I am in this room.

Prospective access is about allowing law enforcement to have access to information that is in existence in telecommunications networks, and it is giving them a near real time so that they can actually investigate crimes. For example, if they have particular numbers under watch because they know a drug deal is going down and they have a belief that a person is in a particular region, be it Sydney at the wharfs to collect something or at a post office roughly in a geographic area, they can use that with other technology that they currently use under surveillance devices to find whether someone is at a place at one time. It may be possible in the future, if industry develops this technology, to pinpoint people; this provision might give that sort of access. But that is something that is certainly a futuristic type situation.

In the comparison between surveillance devices, Commonwealth legislation, what we are proposing here and what currently happens, the Surveillance Devices Act, in providing a warrant, is in effect giving you power to trespass upon a person or a place to implement a device that will then be used to track someone. In relation to a mobile phone, to get a tracking device or get a surveillance devices warrant on a mobile phone, you would have to get some sort of technology that you stick onto the telephone to actually follow the person. That is not capable of happening under a surveillance devices warrant at the moment, because a surveillance devices warrant is all about applying something to a person, to a car, to a place or to a parcel. A tracking device, under the Surveillance Devices Act, is similar in that it allows law enforcement, the Australian Federal Police and the ACC, with the authorisation of a senior officer within that agency, to track a person where there is no trespass involved. They

can follow that person, do certain things and use optical where they are not attaching something to a person.

To access prospective information in nil to real time, you need the assistance of the telecommunications provider. It has been the policy that, with any assistance that is needed from a telecommunications provider, there can be no interference by law enforcement without the assistance of the actual provider involved. That is the reason that it would sit within the TIA act rather than within the Surveillance Devices Act.

Senator LUDWIG—With respect to assisted GPS technology on mobile telephones, at the moment we think of radials around a mobile site, say, at Brackenridge. They can already detect by the strength and weakness of the signal how far away you are on that radial. It does not take much to then pinpoint you on that radial with another intersecting line, if you have sufficient technology or new technology to be able to intersect that line, to say whether you are on this side of the radial or that side of the radial. When you have an intersection of the two lines you know precisely where you are. That type of technology is currently being mooted to be introduced in 2007-08. If that is the case, you then ask the provider to provide information, for argument's sake, in near real time what that data stream is—in other words, what those coordinates are—and that will then give you the location of that mobile phone. It does not have to have a device attached to it. If that is the case, you can ask for a 45-day warrant for the mobile phone. You can then ask the internet service provider, if they have the technology, to provide in near real time where that device is by that system of coordinates, and they can then update that literally by the minute to detect where that mobile phone is and where it is going. And we assume they have a unique identifier of the mobile phone so they know the person who might be carrying it. That seems to be the concern of the EFA. I am not sure that you addressed that point.

Ms Smith—From our perspective that is addressed by the fact that we have acknowledged that there is potentially a greater breach of privacy if a person can access prospective data, and that is why we have separated it out from historical data. We have placed a time limitation on it. We have also limited the agencies that can access this information to criminal law enforcement and national security agencies, and we have made it an offence that is punishable by three years, which is consistent with the surveillance devices legislation.

Senator LUDWIG—The argument seems to be from the EFA that it is an easier process to obtain that prospective data from the ISP than it is to obtain a surveillance device. In other words, the procedure should be the same as their fallback position. Do you agree or disagree with that?

Ms Smith—I do not agree, because I believe that we are establishing certain hurdles that they will have to get through to access this information. There is also something called the Communications Access Coordinator's determination, in which we will prescribe all of the hurdles that an agency must go through before they can obtain this information and the kind of form that it has to be in. We will dictate fairly stringent guidelines for how this information is accessed. We obviously do not have any guidelines at the moment, because that is something that will be developed. That relates to section 183 of the bill, which talks about the kind of information that we can put into these standard authorisations. I think it is equivalent to the tracking devices underneath the Surveillance Devices Act, namely, that a senior officer

within the Australian Federal Police can obtain one of these prospective warrants. It is an authorisation and not a warrant in both cases. If we are talking about tracking, certainly the AFP can track now with one of these authorisations. As far as commenting on the capabilities of what might be available in the network—

Senator LUDWIG—I am only guessing.

Ms Smith—I was going to say, firstly, I do not know and, secondly, I would not comment on capabilities, anyway.

Federal Agent Lammers—As you know, we can already track mobile phones pursuant to the Surveillance Devices Act. That is the physical method of locating and tracking a mobile phone. The thing that has interfered with our ability to do that has not been a technical ability but an ability to get information in near or close to real time from the carriers. That has always been our obstacle. You might remember the AFP saying before that the technology already exists to do this, but it is just not possible given some of the constraints from the carriers. With the emergence of technology the carriers now have the capacity to provide the Australian Federal Police and other law enforcement agencies with that information close to real time. We see that as little more than police's ability to perform its normal function—a tool of the trade, if you will—and not elevated to anything that is possibly captured by the T(IA) Act, which is why it has been removed. The Surveillance Devices Act gives us the ability to track a mobile phone and a number of other targets, and these amendments give us access to the information, because if not for this information then we could not even track the mobile phones. The internal authorisation process that has been established for the Surveillance Devices Act we say is at sufficient threshold to allow us to get access to the data that the telcos currently have.

Senator LUDWIG—Are you saying that they are related but distinct matters, that one is about the actual device and surveillance devices and one is about access to the information?

Federal Agent Lammers—That is exactly right. Up until now we have been able to do what we do in terms of tracking or, more accurately, locating a mobile phone and then following that mobile phone using historical data. The difficulty there is by the time we get that from the telcos the person whom we are tracking or trying to locate may be well outside the cell site that you spoke about just a moment ago. In times of emergency it makes that real time tracking very difficult and cumbersome. So, with the advent of technology and the way the carriers have moved on, we now have the possibility of locating and tracking mobile phones. This is much easier than in the past, and with the safeguards that we are not accessing any of the content associated with any messages that might flow backwards and forwards from a mobile phone. It is just the information that allows us to locate that in a geographical sense.

Senator LUDWIG—The CrimTrac agency is now being sought to be included to apply for stored communication. What was the basis for CrimTrac being included?

Ms Kelly—They are not an enforcement agency for stored communications. They are an enforcement agency in terms of telecommunications data. That is an existing provision under the Telecommunications Act. You may be aware that CrimTrac had a name change from the National Exchange of Police Information, which was existing. At this stage we have

transferred over the agencies provided within the definition of 'enforcement agency' under the Telecommunications Act and we are looking to see whether or not it is appropriate that they continue to be within that definition. Until such time as we can actually establish that it is not appropriate, we have not removed them.

Senator LUDWIG—That was on the basis of their role and function from whence they came. But can you say clearly that they cannot apply for stored communication?

Ms Kelly—They cannot apply for stored communications. I believe they have a role in terms of accessing data for some state and territory police organisations but we are working through those issues.

Senator LUDWIG—With respect to stored communication, my recollection of that bill was that it ultimately came down to what was overt and covert. Covert was said to be an appropriate use of stored communication. In other words, you could not access it at that point. Does this bill change that in any way regarding the near real time data obtained?

Ms Smith—No. The near real time data only has to do with data that is not content.

Senator LUDWIG—Is it the content that would then be subject to the stored communication warrant?

Ms Smith—That is correct.

Senator LUDWIG—Is it still subject to the stored communication warrant?

Ms Smith—Yes.

Senator LUDWIG—It is still not covert and is not affected by it?

Ms Smith—Access to stored communications is covert to the extent that the law enforcement agency goes directly to the provider and accesses it, so that is unchanged. If they want that information in near to real time then they have to do an interception warrant.

Senator LUDWIG—Whilst it had not been delivered it was in the transitory stage, before delivery, and then they would require a warrant?

Ms Smith—Yes. They would require a warrant in both circumstances once it was delivered as well if they wanted to get it from the provider.

Senator LUDWIG—That is the content?

Ms Smith—That is correct. The other information—

Senator LUDWIG—That is the call data?

Ms Smith—If they only want call data, then they can go down the third limb. If they want content and call data they have to go to the higher threshold.

Senator LUDWIG—I raised this earlier but perhaps you can resolve the matter for me. There are probably many explanations but I would like to hear them from you, Ms Smith. Page 13 of the explanatory memorandum, where it deals with secondary disclosure, says:

For example, if during the course of an investigation in relation to taxation fraud, the Australian Taxation Office obtains telecommunications data that concerns drug trafficking ...

Does that presuppose that they have already admitted their occupation of being a drug trafficker to the ATO?

Ms Smith—That would be one reasonable answer. It is possibly more likely that, as part of the investigation, they have found that they have an enormous amount of money—

Senator LUDWIG—There is no other conclusion; they did not win Gold Lotto?

Ms Smith—that they have received information about whom they called with the numbers and that sort of thing; it may be a known drug trafficker they are dealing with and they feel that the information should be passed on. In fact I did listen to that evidence before I left the office, and there would be no way that the Australian Taxation Office would have any content, so it would obviously be very difficult for them to decide that it relates to a drug trafficker. There would have to be information in those numbers they have called or perhaps there were internet sites they visited—if they are making calls to Columbia and that sort of thing—which would give rise to a presumption that that information is to do with drug trafficking. Another possible, more sensible, example may be that, if they have information about particular websites they are visiting and that has to do with child pornography, it might be referred on to the Australian Federal Police for investigation.

Senator LUDWIG—That is what came to my mind as a more practical example, rather than drug trafficking, where you could have a clear relationship with the crime.

Ms Smith—Indeed. In fact we are looking at amending the EM in a couple of other cases, and I think we will pick that one up.

Senator LUDWIG—It just seemed to me that they would have to have the occupation, and I presume the ATO may have already passed that information on if that was recorded.

Senator PARRY—We had some evidence earlier today from the Australian Mobile Telecommunications Association that clause 187(2) of the bill may extend to information that they will not have in their possession. Did you hear that evidence at all?

Ms Smith—Yes, I did hear that evidence.

Senator PARRY—Do you want to make any comment on that?

Ms Smith—I think what they were referring to was being asked by law enforcement or by the Attorney-General's Department in developing interception capability to provide assistance on something outside their network control, whether it be an overseas provider or whether it be a handset provider. The comments that I would make are that you may be aware of some recent amendments that an agency can access a warrant to intercept an actual handset, an IMEI, but there has to be a relationship between that IMEI and the INSI, being the sim card, so law enforcement will seek assistance from a provider in relation to a handset but they will not ask them to dissect a particular handset manufacturer's new handset to see all the technology in it, they will only ask to the extent that they are providing a service over that.

Senator PARRY—There would be no penalty or imposition upon the provider if they cannot provide information that is not within their realm to provide?

Ms Smith—That is correct. It is only with regard to the intercept capability over services within their control. Of course, they have control in their network over services that are not

handled by them because they have commercial relationships with smaller providers to carry their traffic. We would seek their assistance on occasion on those ones.

Senator PARRY—Thank you. I refer to clause 188, concerning delivery points. I am still not sure of the department's position and why the department wants one point of access or control of access points or delivery points. I have read the EM, and it seems to be a fairly important point. Can you explain the reasoning behind delivery points: why there is a control over where the delivery points shall be and the right of the CAC to say that they do not approve of a particular delivery point, that they want a better delivery point? What is the reasoning?

Ms Smith—I will pass to my colleague, Mr Markey, but first off I will say that we moved the provisions over from the current Telecommunications Act, as they stand.

Mr Markey—To clarify the delivery point: the first step in deciding the delivery point is that the carriage service provider decides where that delivery point is, so they make that decision.

Senator PARRY—Is the delivery point the place or the location where the information provided is transmitted to the agency requesting, or is it where the information that is intercepted is first obtained? What is the delivery point?

Mr Markey—If you refer to the diagram provided, it would probably better explain delivery points and the interception capability and delivery capability. Interception capability obviously happens within the domain of the carrier at certain points within their network. It was decided for a telecommunications service that an agreed delivery point to deliver that intercepted data be delivered to that delivery point and then be mediated by the delivery capability before then sending it on to the intercepting agencies.

Senator PARRY—What do you mean by mediated?

Mr Markey—Mediated is with regard to the format of the data. For example, the interceptor putting in headers saying, for example, 'warrant ID'.

Senator PARRY—Presented in a reportable form?

Mr Markey—Exactly.

Senator PARRY—It has nothing to do with the physical interception. It is just a location where it is put into some form that can then be delivered to the agency requiring it?

Mr Markey—Yes. It is also a cost demarcation line of the obligations of the carrier and also the obligations of the government, of who pays for interception capability and who pays for delivery capability.

Senator PARRY—I think we are getting to the crux of the matter. My final question is on costs. How are you going to determine what is a fair and reasonable cost that the operator or agency will charge?

Ms Smith—It is interesting that you say that. That is often the complaint of both industry and agencies alike: what is a reasonable cost. There is an arbitration role that ACMA can undertake if either side is unhappy with how that is determined. Essentially, in relation to the provision of this information, contracts are developed between the agencies and the carriers in

relation to the interception capability. In relation to call associated data, there tends to not be any contracts in place; it is based on the actual cost to the carrier. For example, if someone were to be called out at midnight on a public holiday, the costs for that are much higher. It is based on the costs that the carrier has to actually physically pay that person as well as going into that part of the infrastructure, because they get their money back on what they have spent. The premise in the Telecommunications Act is that there should be no profit or loss on the part of either party. There have not been complaints about this where they have been prepared to take it to ACMA, from either side. It is an area that we often provide advice on and suggest that matters are referred. I checked with ACMA last week to see if they have had anything referred to them in the last couple of years, and there have not been any.

Senator PARRY—At a different committee and a different format, we were discussing costs and a commissioner of police indicated that it was a fairly substantial cost to his agency to undertake telephone interceptions. Are you saying that it will only be cost recovery for labour and it will not be return on investment or return on infrastructure components?

Mr Markey—As far as the agreement between the Commonwealth and the carrier is concerned, it is on a carrier basis and it includes the cost of infrastructure, the labour, the project management, the administration and the logistic costs, probably up to periods of three years, of maintaining that capability.

Senator PARRY—Do you feel that these costs are fair and reasonable?

Ms Smith—We are not involved in the costs at all. As I have said, ACMA holds that role quite clearly as arbitrator so we refer any concerns to ACMA. We do not make comment on that.

Senator PARRY—Your evidence is based upon the fact that there is really no complaint and that it seems to be working smoothly as it currently exists. Will the costing arrangements under the new provisions stay the same?

Ms Smith—There has been one very minor change under the costing, and that is that we have made it clear that anyone who gets access to call associated data from a carrier for whatever reason must pay. In the past some Commonwealth and state agencies have sought information under the powers of their own legislation and have not paid for that information. Law enforcement, who always apply under certain provisions and certain Commonwealth agencies, have always paid. We are amending it in this bill to make it that everyone pays.

Senator PARRY—It is fairer and more equitable?

Ms Smith—Yes, it should be fairer and more equitable.

Senator PARRY—The industry should be happy with that. Do you anticipate an increase in interceptions under the new provisions or just business as usual?

Ms Smith—I would say business as usual.

Senator PARRY—Finally I turn to the cost side of it. You have the delineation that the agency costs are basically up to the delivery point and the costs on the carrier are when you do the physical handover—at that point the costing stops. Are there any other costs involved that industry would have to bear?

Ms Smith—No, other than the legal costs in negotiating contracts with the Commonwealth.

Senator PARRY—Does that happen very often?

Ms Smith—No.

Mr Markey—With regard to negotiations for contracts, the lead agency negotiates contracts on behalf of the government with a number of carriers or carriage service providers to provide delivery capability from that delivery point.

Senator PARRY—Thank you.

Senator KIRK—I have a few questions arising out of the evidence given to us today by the Australian Mobile Telecommunications Association. They have suggested that there be an amendment to schedule 1, item 11 of the new section 6R, regarding the requirement for CAC to take into account the objects and regulatory policy of the Telecommunications Act. They suggest that amendment in order to clarify matters. I wonder what the department's view is about that.

Ms Smith—Our view is that that is unnecessary. The objects of the Telecommunications Act are picked up under several of the powers of the Communications Access Coordinator, also known as the CAC. There are particular provisions where the minister can make determinations in relation to interception capability plans. The objectives of the act are picked up there. The applications for exemptions and the objectives are picked up there. We feel that the decision-making powers that the CAC has refer implicitly but we have made them explicit in particular of the provisions. You will note that those provisions have also picked up the interests of national security and law enforcement and particular ones have picked up the interests of privacy, and there is a required consultation with the Privacy Commissioner. We feel that they are already in there. The role of the CAC is to make decisions on behalf of law enforcement—national security—in relation to particular things, so we are not sure that it would add anything. The definition, except for the change of the name from the agency coordinator, is exactly as it has been since 1997 and it has worked extremely successfully.

Senator KIRK—They also had some difficulties with the definition of 'interception capability' in the bill. Did you hear what they had to say about that?

Ms Smith—Yes, we did.

Mr Markey—In going back to the diagram, the interception capability refers to the carrier or carriage service provider having the capability to intercept the telecommunications service and deliver it to a delivery point. It is in regard to any telecommunications service that they provide that that service should be interceptable.

Senator KIRK—They are concerned that it would extend to handsets which are not within the control of the carrier and/or applications hosted overseas.

Mr Markey—AMTA were talking about customer premise equipment and they referred to the Telecommunications Act. Within the Telecommunications Act 'customer premise equipment' refers to the equipment that resides within the premise of the customer—for example, mainframes, network terminating units, routers and switches. They gave examples of how in the new technology age these are becoming less in control of the carrier. In our

view in some cases in the industry they manage or remotely manage those routers, switches or mainframes. Therefore, we believe with regard to the definition under the act that the physical location does not dictate whether or not the equipment is under the control of the carrier.

Senator KIRK—What about a mobile phone handset—that is not within the control of the carrier?

Mr Markey—That is correct. I will redefine that. If it is not in the control of the carrier then they have no obligation.

Senator KIRK—I see. So that control element is taken into account?

Mr Markey—I believe so.

Ms Smith—Except to the extent that a handset is connected with a service and that the provider is intercepting on behalf of the agency, they can intercept on the handset. There is a warrant that lawfully allows them to intercept an IMEI. To the extent that we need their assistance in relation to intercepting the handset that is connected to one of their services, we seek that assistance. What we do not ask them to do is to provide us with information on how to intercept a handset. A handset is of no significance unless there is a service attached to it.

You also mentioned overseas providers. The reality is that many providers in Australia are currently rolling out overseas services that they purchase overseas and repackaging them as their own. To the extent that they repackage it or badge it as a particular phone service of their own, clearly they will have to provide assistance with that. There is an exemption regime if they are unable to assist law enforcement—they go to the CAC and the CAC will consider their request. The underlying premise of this is that it is not an opt-in system interception capability; it is an opt-out system. All services on an equal, level playing field must have interception capability unless currently the agency coordinator, and in the future the CAC, decides for certain reasons, including the objects of the Telecommunications Act, that interception capability is not viable in that case.

Senator KIRK—I wanted to ask about exemption power. AMTA also suggested that there should be some kind of cap or time limit on the period during which a refusal of an exemption by the CAC under section 193(6) can take place. They were suggesting a period of 180 days. I understand that at the moment it is unlimited.

Ms Smith—No. An amendment came in a few years ago to the Telecommunications Act that places a 60-day time limit upon the agency coordinator to make a decision in relation to an exemption. The reality is that all decisions are made well within those 60 days. The 60-day time limit is a limit upon the department to actually administratively move this forward and make a decision. If after those 60 days the department has not made a decision in relation to that application then there is an automatic exemption granted so that a carrier will not be in breach of the legislation, because if it was automatically granted that no exemption existed then they would be in breach of the legislation. The situation is such that when any application for exemption is made, if it is a complex one—if there is a potential that an exemption will not be granted—we engage immediately with the provider so that there will be no potential surprises. We try to work with them to come up with a solution if we believe that they strongly need interception capability. What was not mentioned in the evidence from AMTA or Telstra—I am not sure which one it was—was that we seek that the providers ask

for an exemption from their capability prior to the rollout of that service, because we do not want to slow down the rollout of services and that sort of thing. If it can all be done prior to the rollout of service then there will not be that 180-day concern that they are talking about. We do not ask them to retrofit; we ask them to talk to us in advance of rolling out a service. They all know they have to have capability. If they cannot meet it or for some reason they think it is not appropriate, we want to work with them on the exemption issue. There are many compromises, which I would not want to go into on the public record but I could go into in camera, as to how we would work that exemption process.

Senator KIRK—The matter really should not arise?

Ms Smith—No. I asked my staff before I came out if we had had one in the last two years that went over the 60 days and the answer to that was no.

CHAIR—Some witnesses here today have talked about the consultation process. Are you happy with the consultation process, that it has picked up the different measures and amendments that needed to be made and that they have all been addressed and taken into account?

Ms Smith—There has been exceptional consultation on this particular bill. We have had a very broad-ranging level of consultation and a lot of that is because we now have a branch within the department that is putting resources into spending much time with our stakeholders. I will pass to Mr Curtis, who ran our consultation process, to talk about it. Essentially, the only comment I would make is where it is clear that there is an impasse and we need to do a lot more work, we prefer to move the provisions over as they are in a standard form that has been accepted for 10 years rather than try to change them at this point. In talking to our stakeholders we acknowledged that more work would be needed in the longer term on that, and standards was the case that was mentioned earlier.

Mr Curtis—In the first place we developed the draft legislation in close consultation with Commonwealth government agencies. That was an internal consultation process. We released the exposure draft of the bill in February and we received 32 submissions addressing the various provisions. To follow up on that we also had a number of meetings and conversations with industry groups and various submitters to work through some of the issues that they raised. Quite a few of the issues that they have raised have resulted in amendments between the exposure draft and the one that was subsequently introduced.

CHAIR—I note that we have received a couple of later submissions. I am not sure whether you have had a chance to have a look at them. They include the Law Council, Western Australian Police and the Office of the Privacy Commissioner. I will draw those to your attention. If there is anything in them in particular that you would wish to draw to our attention, please do so. The Office of the Privacy Commissioner recommended that there should be a provision inserted into the bill to mandate the destruction of any call data voluntarily disclosed to ASIO. I was just wondering if you had a view on that.

Ms Smith—If we are going to provide comments on each of the submissions then we are more than happy to include that. There are destruction provisions within the TIA Act relating to interception and some stored communications. We have not really turned our mind to

destruction. We have turned our mind to making an overarching piece of legislation and passing elements over from the current Telecommunications Act.

CHAIR—The privacy issues are obviously equally as important. I will just go back to an answer Mr Curtis gave earlier to a question from Senator Ludwig about the Police Federation's concerns about pecuniary interest. We have the response from the Attorney-General in that letter that was referred to, but could that definition of 'pecuniary interest' be narrowed to perhaps just focus on exempting disciplinary proceedings for those police officers concerned? Or can the definition of 'pecuniary interest' just be narrowed to some degree? Has any thought been given to that? The Police Federation were fervent in their views to the committee earlier as to the importance of this to their members. I am happy for Mr Lammers to respond as well if he wishes.

Federal Agent Lammers—I cannot comment directly on the PFA's comments. However, from the Australian Federal Police point of view, we do not have a problem with any system that adds accountability to our processes.

Mr Curtis—In general terms it would not be appropriate to exclude pecuniary penalties overall. Obviously under some of the individual state and territory police acts some of the pecuniary penalties that would trigger the secondary disclosure provisions would be quite serious. Given that 'pecuniary penalty' is a fairly broad term, the alternative would be to try to insert more detailed definitions that relate and encompass all those different state and territory police acts. Before we did that we would need to consult closely with each of the state and territory police commissioners. It should also be said that, because the definitions in question that are giving the Police Federation trouble are in the state and territory legislation, our view is that it is probably better that they deal with it as a matter under the state employment legislation. Many of the police employment acts do not contain pecuniary penalties. I understand that the AFP is one of those, so it is very broad.

CHAIR—They indicated two jurisdictions. AFP was one and I am not sure what the other one was but it did not include a pecuniary interest provision. Thank you for your feedback. I know Mr Curtis has the ability to consider both sides of the argument, having been on this side of the table and now on that side of the table.

Mr Curtis—I have been well trained in this.

Ms Smith—He has been.

CHAIR—We appreciate your impartiality. You have answered some of the questions from EFA. EFA also raised the definition of content and data with regard to web browsing and the internet. If you are looking at a site and it tells you about a certain event on a certain date, it is pretty clear what is going on. From my perspective it appears that there is a possible blurring of the definition. Do you see that as a concern, that it is problematic or not specifically?

Ms Smith—We are thankful to EFA because they picked up a problem with the EM, which we will correct. On one page we say, 'URL is content' and then on another page we say that it is not. So we will certainly clarify that. In relation to getting call-associated data regarding an IP address that can identify a web page, that is not content because all it does is tell a law enforcement agency that a certain target went to a certain website. It does not tell them any other details. It does not tell them that they then went into their bookings online or via their

travel agent or that they downloaded particular information. It does not give them any knowledge of the substance as to why they were on that web page. URLs are a little different because they will then point out the continuum of where the person actually went to. Mr Markey is the technical person, so I will ask him to comment on the differentiation. But I will just say one other thing. It is very important that we keep this technologically neutral. Every day a new technology comes up, a new name comes up. We generally talk about metadata, which is all of the information that is not content, but what I would assure the committee is that we do provide legal advice to law enforcement and to industry alike. They will come to us when they get a warrant. They will come to us when they get a request and they will say that they are concerned about it. We will take any new technology on board and provide advice as quickly as we can on these particular issues.

Mr Markey—With regard to web URLs—or URIs—and how an apparatus finds that on the internet, I will go back to the analogy of when we used to make telephone calls; if we had call charge records we would have a list of numbers that a person called but it does not show content. It is the same reason with the URL. It would have a web server log with a list of URLs and by that nature it does not show content, it just shows a list of URLs. If an officer wants to phone those numbers and find out what they are they could ring them systematically. It is the same with a computer. When they go and click that button to search that URL, it is the same thing. The request is done automatically from that PC to a domain name server or system to find that URL over the internet. But it does not actually look at content; it is just trying to find that address within the internet.

Ms Kelly—A practical example of that is: if you have call-associated data from a telephone call and you find the number is associated with, say, the Medicare office, when somebody is looking up the Medicare office on the internet the call-associated data is the same thing. It just provides you with the information of who that person communicated with, whether or not it is the Medicare telephone number or the Medicare home page, so it is very much akin to that.

Ms Smith—But that access and that information that you get, that IP address, does not give them a glimpse of my typing in my Medicare number and my claiming back a doctor's appointment on 6 December. It does not give any of that information. Another example would be that you went to the library and borrowed a book. It does not tell you what page you were reading. It just says that you have an interest in a particular book, which is publicly available information. We are very careful to ensure that no content whatsoever is available under these provisions. There are two very strong regimes for access to content, being stored communication and intercept. We are very, very careful about that.

CHAIR—You have been asked questions about CrimTrac. That has been an issue that has come up today on a number of occasions. Concerns have been expressed that it is not a law enforcement agency, but nevertheless the information is being transferred over. You have answered that. I will have a look at the *Hansard*, but if there is anything further that you wanted to do to alleviate any concerns about that issue, that would be appreciated.

Ms Smith—We are dealing with CrimTrac. We need to go back to the basic policy of why they were placed in there in the first instance. That is something we are certainly working on and, again, we thank those who put in the submissions for bringing it to our attention.

Mr Curtis—We have sought clarification from them already.

CHAIR—What is your position then on CrimTrac?

Ms Smith—We do not have a position yet because we are still working on it. They gave us some information, and we have gone back to them to say, 'On this basis, should we recommend your removal from this system?' They are obviously talking to the head of CrimTrac. Again, this is one of those historical situations where NEPI was given access by the communications department some years ago, so we need to go into that further.

CHAIR—Are we likely to get an answer in the near future?

Ms Smith—We will be responding to the different things that have been raised in that, so we hope to be able to give you something on that.

CHAIR—Thank you very much for your evidence today.

Committee adjourned at 5.06 pm