



COMMONWEALTH OF AUSTRALIA

# Official Committee Hansard

## SENATE

LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE

**Reference: Telecommunications (Interception) Amendment Bill 2004**

MONDAY, 22 MARCH 2004

CANBERRA

BY AUTHORITY OF THE SENATE



## **INTERNET**

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

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

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

**WITNESSES**

**GRAHAM, Ms Irene Joy, Executive Director, Electronic Frontiers Australia Inc..... 2**

**HOLLAND, Mr Keith Colin, Assistant Secretary, Security Law Branch, Attorney-General's Department ..... 19**

**LAMMERS, Federal Agent Rudi William, Manager, Technical Operations, Australian Federal Police ..... 12**

**LAWLER, Federal Agent John, Acting Deputy Commissioner, Australian Federal Police ..... 12**

**PHELAN, Federal Agent Michael Anthony, National Manager, Border and International Network, Australian Federal Police..... 12**

**RYLES, Mr John Ashley, Manager, Information Technology, Australian Federal Police ..... 12**

**SMITH, Ms Catherine Lucy, Principal Legal Officer, Attorney-General's Department..... 19**

**TEARNE, Ms Anna, Principal Legal Officer, Security Law Branch, Attorney-General's Department..... 19**

**WOODLEY, Mr Stuart Robert, Senior Legal Officer, Attorney-General's Department..... 19**

---

**SENATE****LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE****Monday, 22 March 2004**

**Members:** Senator Payne (*Chair*), Senator Bolkus (*Deputy Chair*), Senators Greig, Ludwig, Mason and Scullion

**Participating members:** Senators Abetz, Brandis, Brown, Carr, Chapman, Eggleston, Chris Evans, Faulkner, Ferguson, Ferris, Harradine, Harris, Humphries, Kirk, Knowles, Lees, Lightfoot, McGauran, McLucas, Murphy, Nettle, Robert Ray, Sherry, Stephens, Stott Despoja, Tchen, Tierney and Watson

**Senators in attendance:** Senators Greig, Ludwig, Payne and Scullion

**Terms of reference for the inquiry:**

Telecommunications (Interception) Amendment Bill 2004.

**Committee met at 9.36 a.m.**

**CHAIR**—This is the first hearing for the Senate Legal and Constitutional Legislation Committee's inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2004. The inquiry was referred to the committee by the Senate on 3 March 2004 for report by 30 March 2004. The Telecommunications (Interception) Amendment Bill 2004 amends the Telecommunications (Interception) Act 1979 to extend the availability of telecommunications warrants to additional serious offences, to extend the protections of the act in relation to text based communications, to facilitate the recording of calls to publicly listed ASIO numbers and to clarify the application of the act to delayed access message services.

The committee has received seven submissions for this inquiry and a number of late contributions. All of the submissions received on time and in agreement with the committee have been authorised for publication and are available on the committee's web site. Witnesses are reminded of the notes they have received relating to parliamentary privilege and the protection of official witnesses. Further copies of those notes are available from the secretariat.

Witnesses are also reminded that the giving of false or misleading evidence to the committee may constitute a contempt of the Senate. The committee prefers all evidence to be given in public but under the Senate's resolutions witnesses have the right to request to be heard in private. It is important that you ask the committee and give notice if you intend to give evidence in camera. I also ask witnesses to remain behind for a few moments at the conclusion of their evidence to assist the Hansard staff with clarification of terms or references.

[9.38 a.m.]

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

**CHAIR**—Electronic Frontiers Australia has lodged a submission with the committee, which we have numbered 1. Do you wish to make any amendments or alterations to that submission?

**Ms Graham**—We do not wish to amend it but we have looked further into some of the aspects of the bill and our fundamental recommendation has changed. We are not saying that anything we have written in the submission is wrong but we are now of the opinion that an interception warrant should remain necessary for accessing stored communications even after they have been read by the intended recipient. I can talk more about that later.

**CHAIR**—All right.

**Ms Graham**—I am just saying that the submission has been overtaken somewhat by further information that has come to our attention.

**CHAIR**—Bear in mind that the committee is limited in terms of time.

**Ms Graham**—Absolutely.

**CHAIR**—We appreciate your submission. I ask you to make a brief opening statement and at the conclusion of that I will go to members of the committee for questions. Notwithstanding the fact that we have started late we will make sure that adequate time is available as was previously scheduled. Thank you very much.

**Ms Graham**—Thank you very much. I will not make a very long opening statement because I am very aware of your limited time. There are a couple of things that I would like to draw to your attention at the beginning. When we lodged the submission, as I indicated in that, we had not had sufficient time to go into enough detail in analysing the effect. Now that we have we have become aware that, in the case of messages that have been read and have been left stored on an ISP server, under various state and territory law access to those messages will be available in some circumstances without a search warrant at all and in other circumstances where a search warrant has only been issued by a justice of the peace or a person appointed by one of the state attorneys-general. We do not think that that constitutes sufficient protection and accountability measures, even for messages that have already been read and still remain stored. We are of the view that there needs to be an interception warrant still necessary or, alternatively, perhaps Commonwealth law needs to be amended so that there is an intermediary type search warrant that, so to speak, covers the field in preventing vast access by law enforcement authorities at a state level, for example.

The other aspect that has come to our attention, which I think was also raised by the Victorian Privacy Commissioner in his submission, is that the stored message changes in section 7(b) and (c) say that once it has been accessed by the intended recipient it can be accessed by anyone else after that. It does not actually limit it to enabling law enforcement authorities to have access to those messages; it just says 'anyone'. It appears to us to mean that, if those messages are still stored on an ISP server, basically any person lawfully on the premises of that ISP can go and read people's stored messages. We feel that there needs to be some further clarification in the legislation in that regard.

I have read the Australian Federal Police submission concerning the employment situation with regard to spam and viruses and things. If the committee would like to discuss that, I am quite prepared to provide some information in that regard. Our interpretation of the existing legislation and the proposed bill suggests to us that the situation would not be quite as dire as the Australian Federal Police appear to think it would be. We think that there may be an issue in the definition of ‘passing over the telecommunications system’. Our understanding is that that telecommunications system may well cease at the boundary between an Internet service provider’s system and a private corporation’s system.

This matter has been raised before in front of this committee in relation to the Cybercrime Bill 2001. I understand that the Attorney-General’s Department advised the committee that a private network probably could not be regulated by the Commonwealth because of the provisions of section 51 of the Constitution. We think that there is a question here as to whether, in the same way that the Cybercrime Act was said not to apply to computers and networks in a private business, the Telecommunications (Interception) Act would in fact apply to email messages once they had been received on the business’s equipment. Unlike a telephone call, once an email message has passed across into the private business network, the communication is no longer on the public network the way a telephone call is. In a telephone call, if there are two people one is clearly speaking across the public network at the same time that it is being received in the business. But in the case of an email message, it is sent from the public network, crosses the boundary from the public network into the office and has then arrived in the office. It is not, at the same time, on the public network. So we think that there is an issue here in terms of definitions in the Telecommunications (Interception) Act concerning network boundaries—that it may or may not be the case that email messages in private businesses are subject to the interception act. That is basically all I feel I need to particularly draw to your attention in an opening statement.

**CHAIR**—Thank you for keeping it brief, I do appreciate that.

**Senator LUDWIG**—In your view, when do you then say that a TI warrant is not required? I want to clarify this first, because you have changed your position. I have read your submission and I thought I understood where you were. You have now resiled from that position. When you then say that a TI warrant for SMS and emails is not required? There are a number of mediums. There is web mail, email and SMS messages as well.

**Ms Graham**—We believe that an interception warrant should be necessary to access any messages that are stored on an ISP’s own equipment on their premises where it is possible for law enforcement agencies to go into those premises, without using a telecommunications system, and access those messages. I am aware that the Federal Police submission, for example, suggests that web mail is somehow different. Web mail is not different from any other kind of email: the messages are still being stored on an Internet service provider’s mail server on their premises and it is being accessed over the web the same as you access a message with Microsoft Outlook or whatever. So the messages will always be stored on an ISP’s premises. Our view is that, when the messages are stored in the ISP or the telecoms voicemail system on their premises, an interception warrant should be necessary. With regard to an SMS message, our understanding is that, when the SMS messages have been delivered to the intended recipient, they are stored on the SIM card in the mobile phone. Once it has

been received by the intended recipient, we have no problem with police being able to access that with an ordinary search warrant, because it is no longer stored on the ISP's premises.

**Senator LUDWIG**—Just on that point—and I hope you will be able to hold your train of thought and come back—if, when you execute a general search warrant on a residence, you pick up the mobile phone handset and it is turned off and you turn it on, it will then pick up any incoming messages, so they will then transfer at that point.

**Ms Graham**—Yes, that is a very interesting question, if the phone is turned off and you turn it on. I agree with you entirely, Senator. I had not thought of that.

**Senator LUDWIG**—What is happening is they have got to the handset, and you say in your submission that they are then capable of being read.

**Ms Graham**—Sorry?

**Senator LUDWIG**—You have just said that you have no problem with them being read once they have been stored on the SIM or the memory. If it has the flashcard in the handset, it is okay to be read but, if the phone is off, the act of turning the phone on will instigate the recovery of any messages that are outstanding, at which point the handset can then be read to see if there are any ingoing or outgoing calls depending on how the user has utilised the telephone. Is that okay too?

**Ms Graham**—No, we do not think that is okay. Perhaps I can explain our core position, which is that we believe an interception warrant should be necessary until such time as the intended recipient has had the opportunity themselves to read the message and delete the message if they wish to. Basically, it is the same as if you have a telephone call and, at the end of the telephone call, it is gone. We believe that people should, using email and SMS, have the opportunity to have private conversations and delete the message when they have finished the conversation and that it should not be accessible without an interception warrant. In the case that you have just explained as to how a law enforcement agency could turn on the mobile phone and, in that way, receive messages—

**Senator LUDWIG**—They could ask the owner of the phone to turn it on.

**Ms Graham**—That is right, yes. Again, we would say that those messages should not be accessible without a telecommunications interception warrant, because they are not being firstly received by the intended recipient.

**Senator LUDWIG**—What if they have asked the recipient to turn on the phone and the recipient has obliged?

**Ms Graham**—We would say that it has to be voluntary on the part of the recipient, and it would clearly not be voluntary if you had people in your home or whatever with a search warrant. In my opinion, that would not be considered to be voluntary. We feel that it would need to be completely voluntary and that the person gave them the information. If it has been happening under a search warrant, people will not say no.

**Senator LUDWIG**—What about if the recipient has not read them but they are available to be read on his email service? Right now I do not have my computer with me, but I know where it is and I know that there will be incoming emails all the time.

**Ms Graham**—A telecommunications interception warrant should be necessary, because you have not read those messages and you have not even downloaded the subject lines. You have no idea what is actually there, in principle.

**Senator LUDWIG**—That is not right, though, is it? I can view the content of the email, the by-line and what is in it, by the way I set up the Outlook program, even though I have not actually double-clicked on the email itself.

**Ms Graham**—But if it is in Outlook, you have received it on your computer.

**Senator LUDWIG**—Yes. So you say that then it is all right. But it will still show as unread even though I can have a preview pane.

**Ms Graham**—I am saying that those messages, theoretically, have been downloaded from your ISP or wherever; they are on your computer and you know they are there. If you have not read them, our view would be that that is your problem. If the police have a search warrant to come into your home or office and search the computer and read those messages, we do not have a problem with them using an ordinary search warrant, because, clearly, you have downloaded the messages and they are in your possession. It is different if copies of those messages have been left stored on your ISP's server and you do not know that they are there—or even if you do know that they are still there. As we said in our submission, if they have made copies of everything in the course of doing backups for disaster recovery, there are going to be copies of those messages still stored at the ISP and they could be stored there for three months. If that has happened and you have not had the opportunity to delete them, we believe an interception warrant should be necessary to access the ones left stored on the ISP's server. But for the copies that you have on your computer that you know are there, we say that a search warrant is acceptable.

**Senator LUDWIG**—So if they execute a search warrant now on my premises at home—I will not use parliament as an example—and there are unread messages, you say that a TI warrant is not required, even though I have not had an opportunity to read them?

**Ms Graham**—Yes. We would much prefer that a TI warrant was required.

**Senator LUDWIG**—I just had to resolve that.

**Ms Graham**—We would say that if you are going to try to draw a line then clarify the law more than what it is now. To us the line needs to be drawn where the person has at least had an opportunity to read the message. If they have chosen not to read it, we would accept that there is a limit to how much privacy you can expect to have.

**Senator LUDWIG**—But I do not have an opportunity to read it. I have broadband at home and Outlook is running pretty well all the time. I am here for a week. I execute it tomorrow or today. I have not had an opportunity.

**Ms Graham**—I would be quite happy to agree that an interception warrant should be necessary always.

**Senator LUDWIG**—I am trying to stop you running away on me and I am trying to pin down, if you do not mind, what you are now saying. I have got in writing what you say your position is, but I do not have your position now. It appears to keep running away on me.

**Ms Graham**—The problem is that I think you are quite right: there are so many different circumstances—

**Senator LUDWIG**—I am not right; I am just posing different scenarios.

**Ms Graham**—Sorry, I mean right terms of giving a range of examples as to how people actually access email. There are so many ways that people use email and so many different circumstances to do with when and how they access it that it becomes difficult to identify exactly where the line is drawn. That is why it probably sounds like my position is a moving feast.

**Senator LUDWIG**—It does, frankly. I am happy not to be critical about that. I am just trying to establish what it is. The other difficulty is MSN or a message service. When the computer is on, it will run automatically. So my broadband and web based email will be running automatically, and as the messages come through they will be stored.

**Ms Graham**—Sorry, which system?

**Senator LUDWIG**—Outlook is the more traditional email service. There is also a message service which will run with broadband simultaneously when you are online so that you can literally have a two-way conversation as you email someone.

**Ms Graham**—Are you talking about one of those chat—

**Senator LUDWIG**—No, it is not chat; it is different again. It is a message service, instant messages that come online.

**Ms Graham**—I am with you now.

**Senator LUDWIG**—So the same thing occurs in that they will keep popping up all the time. You might want to go away and think about some of these issues.

**Ms Graham**—I think that the EFA board's position would be that, short of legislating in a way that identifies every single circumstance where a message might arrive on your computer, it may well be preferable to say that an interception warrant is simply always necessary. That way we can ensure that people's privacy is protected, that there is a limited range of agencies that can invade people's privacy and that it is only used in the case of serious crimes. I think we need to think about it a little more. We had not actually got to thinking about some of the examples you raised this morning; they just had not occurred to us—with everything else to do with the bill. It certainly is apparent that an interception warrant should be necessary even for a home computer connected by broadband, as you say, or at the end of the day law enforcement agencies will be able to access messages that people did not even know they had received. That is the problem that we have: we believe people should have the right to receive the message, the same as they receive a phone call, before anybody else has a chance to read or listen to that message. Because of the different technology, there is this attempt, basically, to get access to people's private communications before the people themselves have even had access to them. Fundamentally, that is our problem in terms of drawing the line. We think an interception warrant should be necessary until the person has had the opportunity to read the message themselves. Does that help?

**Senator LUDWIG**—I am only establishing what your position is.

**Ms Graham**—That is what I mean: does it help in terms of establishing what our position is?

**Senator LUDWIG**—I have a lot of other questions, but I think I should share your time around. You say that the TI warrant should now be required in all instances unless a person has had the opportunity. How do you define ‘opportunity’? Do you mean opportunity in the sense that they have actually looked at the email and checked it?

**Ms Graham**—I think it would have to be that they have actually looked at the message.

**Senator LUDWIG**—How do you establish whether a person has looked at it? For example, I have a preview pane and, effectively, I can read the email and keep moving on without it actually looking like it has been read.

**Ms Graham**—If it looks like it has not been read, they still need an interception warrant.

**Senator LUDWIG**—So even though I have read it and deleted it?

**Ms Graham**—If you have deleted it, they cannot access it.

**Senator LUDWIG**—They can if they go to the ISP.

**Ms Graham**—Yes.

**Senator LUDWIG**—Having previewed an email in the window pane, I can delete it without actually clicking on it and opening it and reading it in the fuller sense. We get a lot of spam. It will come up in the preview pane and I will delete it without opening it. It could also have a parasite or a virus attached, so that is the beauty of some of the modern technology.

**Ms Graham**—Given that the message has been deleted without being read—

**Senator LUDWIG**—But I have, in the sense that I have previewed it.

**Ms Graham**—Yes, that is right.

**Senator LUDWIG**—But you cannot tell that I have done that. The AFP or another agency is not going to sit over my shoulder to try to determine that.

**Ms Graham**—I am sorry, I do not understand the actual previewing bit. You have clicked on it but you don’t—

**Senator LUDWIG**—No. Outlook comes up with a preview pane.

**Ms Graham**—You are talking about the automatic preview in Outlook?

**Senator LUDWIG**—Yes.

**CHAIR**—You do not have to open the email.

**Senator LUDWIG**—I can scroll through using the preview pane.

**Ms Graham**—We would say then that it would appear that an interception warrant should be necessary to access emails on people’s computers.

**Senator LUDWIG**—So you say that, in all instances, a TI warrant is required?

**Ms Graham**—Yes.

**Senator LUDWIG**—I just needed to establish where you were at.

**Ms Graham**—As there are so many ways and means through which people can access emails and so forth, it is clear that trying to draw any narrower a line and still adequately protecting communications is becoming impossible. That is why we feel an interception warrant has to be necessary.

**Senator LUDWIG**—Thank you.

**Ms Graham**—Just adding one quick thing to that, we note that of course law enforcement authorities are saying that this means a vast number of agencies will therefore never have access to certain emails. In our view, that argument is the same as saying that we should not have protection of telephone calls in the first place, because all of those other agencies should be able to access telephone calls as well. We need to remember that the point of interception laws is to protect the privacy of communications. If the effect of in relation to email is that they will not be able to access some communications without an interception warrant, that is no different from the fact that they cannot access telephone calls, once you hang up the phone.

**Senator GREIG**—It seems to me that as a community and as a parliament we get tangled up in this newfangled notion of electronics, the Internet, the Web and what not. From an EFA perspective, is there any fundamental difference between electronic communications and, for the sake of the argument, surface mail? Do we really need new and particular laws to deal with electronic messages, as opposed to the laws which deal with surface mail? Is there any fundamental difference between accessing someone's email and opening somebody's letter?

**Ms Graham**—EFA's position is that there is a vast difference because our understanding is that most people use email far more like they use a telephone call than the way they use a letter. With email, you are talking about almost real-time conversations. I email you and you email me back, and we go backwards and forwards. You have very casual kinds of conversations that are not necessarily as well thought out as what someone would write in a formal letter. So you have a lot ad hoc, off-the-cuff comments that can be easily misinterpreted when you read them in an email—comments that you would have never written in a letter because generally you would be writing a letter more formally than the quick way you just key in something on the email and send it off. To us, an email is far more like a telephone call than a postal mail letter.

There is also the aspect that, with a postal mail letter, you basically do not leave it in the post office. So the fact that you are leaving messages on an ISP server in the first place signifies another aspect of the difference between the way letter mail operates and the way telecommunications operates. With postal mail, all copies of your old letters are not left stored in the post office. In the letter environment that just does not happen, but it does with email. The whole telecommunications process is completely different from letter mail. We think communications through the various telecommunications need different levels of protection from that for standard letters. That has always been the case to date. We think of email as a continuation of the telephone call environment.

**Senator GREIG**—In that sense, does the EFA philosophy go along the lines of regarding email in particular and SMS interception in the same way as phone tapping?

**Ms Graham**—Absolutely. To us, the reasons why email and SMS should have special protection are exactly the same reasons as for a telephone call. I think another aspect that gets

overlooked is that, in all this talk of law enforcement agencies having access to your incoming email, the people whose privacy would be invaded is generally speaking not so much the suspect but all of the suspect's contacts who have been sending them email. When you go to a suspect's mailbox to search what is in it, you are not going to be looking at the email that the suspect has sent to other people, you are going to be looking at the email that lots of other people have sent to the suspect. It is in fact invading the privacy of other people in the same way that telephone call tapping invades the privacy of people who are not the suspects. That is an additional reason why we think email and SMS need to have special protections, because there are so many other people whose privacy can be invaded by the search warrants.

**Senator GREIG**—You spoke in your verbal submission of the lack of clarity or the ambiguity, as you argued it, in definitions of network boundaries. Has EFA given any attention to coming up with some ideas of how they might be better defined?

**Ms Graham**—No. We simply have not had time to go into it in that much detail. The matter of whether companies would be illegally intercepting emails by doing spam and virus scanning only came to our attention late last week. In fact, I did get a phone call from one employer wanting to know whether we had looked at this situation. That was on Thursday afternoon. So we have not had sufficient time to go through it in detail. There is a situation where the interception act has a number of definitions of telecommunications service, telecommunications network and telecommunications system. Some of those definitions are straight out of the Telecommunications Act 1997 and some of them are rewritten in the interception act.

In the Telecommunications Act 1997 there is some detailed information about where the boundary of the network is. There are a number of different circumstances, but in one instance it would be the MDF, the main distribution frame, between the private company and the telecommunications carriers' network. Whether that boundary is also applicable for the Telecommunications (Interception) Act is a good question. As far as we can understand it, it is uncertain. I recently read the discussion paper written by the Victorian Law Reform Commission on email privacy in the workplace and so forth. In that they say that it is unclear in terms of email whether employers in the workplace can monitor email without breaching the interception act or not because it depends on whether the network that is inside a business is a separate network and a separate system from the public system provided by a carriage service provider.

I am saying that we have not had time to go through this in enough detail to give an opinion. I would doubt that EFA's opinion would even be particularly adequate. We would suggest that this is something that perhaps the Attorney-General's Department needs to provide advice on, as to whether the interception act applies in private workplaces or not. This has been an open question for many years, even in terms of emails just between employees in the office, never mind whether or not they are coming from a member of the public. It would seem to us that this bill might be an opportunity for some clarification to be put into the act as to whether employers are prohibited from monitoring their employees' email or not. It certainly is unclear. There is also an argument that the Commonwealth does not have the power to regulate what employers do with email in their own office. I am not saying that they do not have the power. I am saying that that is what has been raised before as being a possible

situation. Our view is that the Telecommunications (Interception) Act needs to be clarified to make clear the situation in private business premises that have their own mail server.

**Senator GREIG**—With the advent of the new G3 technology and mobile phones that can send and receive images as in photos, would it be your view that the sending and receiving of images as opposed to messages would be captured by the legislation or not?

**Ms Graham**—Our understanding is that they would be covered by the Telecommunications (Interception) Act because, to the best of my recollection, the definition of communication includes images. In fact, I have some definitions here. Yes, under the interception act:

‘communication’ includes conversation and a message, and any part of a conversation or message, whether:

(a) in the form of:

(i) speech, music or other sounds;

(ii) data;

(iii) text;

(iv) visual images, whether or not animated; or

(v) signals; or

(b) in any other form or in any combination of forms.

So it covers everything.

**Senator SCULLION**—Ms Graham, my question relates to those aspects of your submission that dealt with the innocent passage of business continuing, particularly the provisions that related to innocent access to a communication by the intended recipient. You went through that process and effectively indicated that it was your view that a court was unlikely to interpret this in a different way from what the explanatory memorandum indicated. In comparison, with regard to the backing up for disaster purposes you appear not to have quite the same approach. You have recommended that you specifically exclude from definitions in the interceptions act the copying of communications data for the backing up purposes of disaster recovery. It has been put to me in submissions from A-G’s that they consider the inclusion of this provision to be unnecessary, principally for the same reasons that you outlined earlier. Could you indicate why there is a difference in approaches? One is that the explanatory memorandum principally puts the issues fairly clearly, and the intention of the act is in fact not to frustrate the legitimate business use of telecommunications. Automated backup for the purposes of business continuity is not intended to impinge on the act. That is covered in the explanatory memorandum. It just seems that there are two approaches. The first is saying that it is unlikely. But the second approach, while it appears to me to be covered in the same aspect of the explanatory memorandum, has been dealt with differently.

**Ms Graham**—I am sorry, are you saying that the Attorney-General’s Department has indicated to you that it would not be a breach of the existing act for the ISP to back up?

**Senator SCULLION**—Indeed. It is certainly not intended that the act frustrate—

**Ms Graham**—We would probably accept that that may well be the case. We were not meaning to say that it would be definitely illegal; we were questioning whether it would or would not. Part of the broader reason for us making that recommendation in relation to backups is that we are concerned that, with the way the bill is written at the moment, messages that had been backed up by an ISP and left stored on a disk or tape drive would include messages that had not been read by the person and had been collected and stored by the ISP, more or less without the knowledge and certainly without the control of the intended recipient. So we were trying to narrow the field to say that, if the messages have been backed up for disaster recovery purposes, you need an interception warrant to access them. So it was not that we were saying that it was probably illegal for the ISP to back up in the first place; we were trying to say that it needs to be clear that, if it is backed up, it needs an interception warrant.

**CHAIR**—Ms Graham, there may be one or two brief questions the committee needs to put on notice to you.

**Ms Graham**—That would be fine.

**CHAIR**—I am sure we will do that by email—

**Ms Graham**—That would be good.

**CHAIR**—given the tight turnaround we have for the committee reporting process. I appreciate it has been a very contracted appearance this morning, but we thank you for your assistance and thank EFA for the submission.

**Ms Graham**—We thank you very much for inviting us to speak. We would certainly be more than willing to provide the committee with any further information that you may want between now and the end of your inquiry.

[10.14 a.m.]

**LAMMERS, Federal Agent Rudi William, Manager, Technical Operations, Australian Federal Police**

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

**PHELAN, Federal Agent Michael Anthony, National Manager, Border and International Network, Australian Federal Police**

**RYLES, Mr John Ashley, Manager, Information Technology, Australian Federal Police**

**CHAIR**—The Australian Federal Police has lodged a submission with the committee, which we have numbered seven. Are there any amendments or alterations that you wish to make to that submission?

**Federal Agent Lawler**—No, there are not.

**CHAIR**—Mr Lawler, would you like to make a brief opening statement, which I am sure will be followed by questions from members of the committee.

**Federal Agent Lawler**—Yes, thank you. The Commissioner of the Australian Federal Police, Michael Keelty, has a long-standing prior engagement in Sydney this morning and has asked me to extend his apologies for his non-appearance. He values the committee and its work very highly. The AFP appreciates the opportunity to appear before the committee in relation to your current inquiry into the Telecommunications (Interception) Amendment Bill 2004. The AFP supports many of the provisions of the bill, including amendments to extend the definition of a class 1 offence to include all terrorism offences. The ability of the AFP to effectively prevent, detect, investigate and present for prosecution terrorism offences and their financing depends on the availability of appropriate investigation and information gathering capabilities such as telephone interception. This amendment will assist the AFP to fulfil its mandate in preventing and detecting terrorist activity and to secure evidence to support successful prosecutions.

The AFP's concerns regarding the telecommunications interception bill centre on items 5 and 10. This is a complex topic and I will endeavour to present the AFP's concerns succinctly. Item 5 proposes to extend the definition of interception from 'listening to or recording' a communication to include 'reading or viewing' a communication. The effect of extending the definition to reading and viewing without appropriate consideration of the impact on operational and corporate factors potentially weakens the AFP's capacity to protect its information systems from virus and spam attacks through the AFP's inability to scan incoming and outgoing emails. The amendments in item 5 also have the potential to render certain aspects of the AFP professional standards regime ineffective because of the resultant inability to monitor emails that may contain inappropriate content.

At present, stored communications can be accessed under the provisions of section 3L of the Crimes Act 1914 and where law enforcement officers have a lawful authority to search a person or property. Item 10 amends section 6 of the Telecommunications (Interception) Act so that, in future, TI warrants will be required for all access to stored communications. There are two proposed exceptions to that: the first is using the intended recipient's equipment so long as access does not require the use of a telecommunications service—that is, email stored on a

hard drive or messages stored on a SIM card; and the second is accessing a message only after the intended recipient has done so. Use of a telecommunications service is not permitted in this exception—emails stored at an ISP. Unamended, the proposed provisions could effectively place many communications beyond the reach of law enforcement. This outcome has the potential to diminish the AFP's capacity to efficiently and expeditiously prevent, detect, investigate and present for prosecution serious Commonwealth offences.

The Australian Federal Police IT security personnel are analogous to bomb technicians in that they determine the danger of the contents of a package and subsequently determine the path the package should take: whether it be sent on, stopped for further examination or destroyed. Human intervention is required to view messages at agency IT firewalls and risk-assess whether an email should be allowed to enter the system. As a law enforcement agency, the AFP is well aware of the damage that can occur when high-tech criminals penetrate an IT system using viruses, worms, trojan horse programs or other malicious code attached to emails. Human intervention and copying of an email prior to its delivery to the intended recipient is also essential for the retention of effective personnel integrity regimes. In the AFP's view, the proposed amendments will impact on the broader government and private sectors in the same way. Without appropriate amendments, the government and private sectors will be restricted in employing security measures to prevent employees releasing client or corporate information and in detecting and preventing viruses from infecting their information systems. Limiting the ways in which stored communications can be accessed under a search warrant may cause investigative delays or an inability to obtain a TI warrant for certain information. This may result in law enforcement being unable to prevent serious criminal offences, locate important evidence and criminal associates including criminal masterminds, or to secure evidence to support successful prosecutions. I hope that during the course of this appearance we will have the opportunity to detail some case examples that will highlight the operational difficulties of what is proposed.

The AFP is very conscious of the importance of balancing privacy considerations with legitimate operational law enforcement considerations. With this in mind, the AFP considers that the proposed provisions would benefit from consideration of legislative solutions that strike a more appropriate balance. In the case of being able to monitor emails to protect information systems and employee integrity, the AFP would welcome consideration of the regulatory regime, one that achieves the same practical balance between access and accountability, that is set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, which are made pursuant to the United Kingdom Regulation of Investigatory Powers Act 2000. In recognition of the need for the government and private sectors to use the most up-to-date technology to preserve the integrity of their information systems and to ensure proper use of those systems by personnel, the UK act provides lawful authority for interception in certain circumstances.

In relation to overcoming the severe operational difficulties that the proposed stored communications amendments in item 10 of the bill will impose on AFP operations, we would welcome consideration of a possible exemption under the Telecommunications (Interception) Act. This approach would enable the AFP to secure important evidence in a timely manner and, in a best-case scenario, to act quickly in the interests of preventing, for example, a

terrorist incident. In the interests of time, Madam Chair, and to give committee members the opportunity to ask any questions, I seek to table with the committee the remainder of the AFP's opening statement. I would ask the committee that, should discussions move to specific case examples, our evidence be taken in camera where appropriate, due to the possibility of disclosing operational capabilities and methodologies. Thank you, Madam Chair

**CHAIR**—You may table the rest of the statement, Mr Lawler. Thank you very much for providing an apology from the commissioner. We understand that he has a range of important commitments and we always appreciate his and the AFP's assistance to this committee, so I would like to note that. I suspect it probably would not matter how much time we had at the end of the day as it would still not be enough time to try to sort through all of the detail of this particular proposition, but I am interested in the concerns, particularly the operational ones, that the AFP has raised. What consultation was there between the Attorney-General's Department and your organisation in preparing the legislation?

**Federal Agent Lawler**—There has been consultation on a range of matters. I understand that in this particular circumstance time precluded there being the level of consultation that we might have liked, given those considerations.

**CHAIR**—By time, do you mean the two years since the committee last reported on a bill of this nature?

**Federal Agent Lawler**—No, I mean in relation to more recent events when discussion took place on the amendments.

**CHAIR**—Although it is two years since it was last considered, isn't it?

**Federal Agent Lawler**—That is true.

**CHAIR**—I will ask Senator Ludwig to continue with questions but I want to correct an omission that I made at the beginning of the proceedings. The committee needs to accept a supplementary submission from the Attorney-General's Department received on Friday afternoon. We need to move a motion to do that.

**Senator LUDWIG**—I so move.

**CHAIR**—As there is no opposition, the motion is agreed to. Thank you.

**Senator LUDWIG**—In relation to accessing emails—and you might have to stop me if I go into operational areas—the scanning is not only machine based; as part of your integrity measures the internal security people who look after your electronic information might also personally open and scan for inappropriate material. You might do samples, audits and checks like that as well. Is that right?

**Federal Agent Lawler**—It is right, yes.

**Senator LUDWIG**—That is without the recipient knowing about it?

**Federal Agent Lawler**—That may be the case, yes.

**Senator LUDWIG**—So you use a range of measures, including that, as part of your firewall to prevent inappropriate material and parasites—and all the other amazing names we have for such things—entering your system?

**Federal Agent Lawler**—Indeed. An example of that might be in relation to potential pornographic images. There are processes—and my colleague from IT security can expand on this—whereby emails that are unsolicited or solicited, if they meet certain criteria, may be prevented from entering the organisation on the basis that it is likely that they contain such images.

**Senator LUDWIG**—Then they might be opened and checked in any event to see—

**Federal Agent Lawler**—They might be opened and checked to see whether they contain such images. If they do, they will be deleted from the system and there may, in some cases, be further internal processes that occur in relation to that.

**Senator LUDWIG**—That would happen depending on the nature of the email, whether it has been solicited or unsolicited, where it has come from and those sorts of issues?

**Federal Agent Lawler**—Yes.

**Senator LUDWIG**—In relation to section 3L of the Crimes Act, what can you do now? I will lead off with an example. If my computer—I seem to be using the example of my computer—is at home and I am not there, you can execute a search warrant on my residence. If it is has a broadband connection it is always on and Outlook is probably running. You can then access any opened or unopened email. What is the position there?

**Federal Agent Lawler**—My colleagues can assist but my understanding is that we have the lawful authority to access those emails. The advice, as it currently stands from the Commonwealth Director of Public Prosecutions, is that that process is lawful under the provisions of a search warrant.

**Senator LUDWIG**—What is the situation if there is reasonable suspicion about some other thing and you enter my residence without a search warrant?

**Federal Agent Lawler**—One would need to have a search warrant to enter your residence unless that was with your consent.

**Senator LUDWIG**—With wireless communication you do not have to enter my residence. If I am running a local wireless communication network you can stand outside and if my encryption code is not particularly good you can access my internal wireless communication. Do you need a telecommunications interception warrant to do that?

**Federal Agent Lawler**—My understanding is that you would require such a warrant, but I would defer to Mr Lammers—

**Senator LUDWIG**—I was just talking about the range of things you say are permissible now. You can appreciate that the TI bill is supposed to move us one way, but I need to establish what you currently can do or what you think you currently can do.

**Federal Agent Lawler**—Certainly, in the case of that latest example, you would require a search warrant if you were searching a particular premises for particular things that had already been articulated in a written affidavit and presented before a judicial officer for authorisation. There are a number of steps and processes that occur before a warrant is, in fact, granted.

**Senator LUDWIG**—And you will come back to me about the wireless communication?

**Mr Lammers**—Yes. With respect to the section 3L provisions that you spoke about first and the power that the AFP and other police have pursuant to that particular head of search, that really goes to the heart of the AFP's argument with respect to accessing information. The AFP believes that information derived pursuant to a search warrant is information that has completed its passage over the telecommunications system if and when it arrives at the ISP. So that really takes a lot of the heat of the argument as to what happens from the time it leaves the ISP to when it gets to a person's residential address or place of business.

Senator Greig, in his comments, went right to the heart of that when he asked, 'Why do we need other powers when we have powers under the search warrant, particularly section 3L, that allow us to achieve what we want to do?' Under the powers present in section 3L of the Crimes Act, if we are at a premises that we are conducting a search warrant at—and I will move to your second point after I explain this—with lawful power of entry we can do everything necessary, on the advice of the Commonwealth DPP, to extract information, whether it be read or not, from the ISP of the owner of the premises or the person upon whom we are going to execute the warrant. The amendments to the TI act significantly complicate that. It means we would then need to get two warrants: a search warrant to enter and search and, if and when we discover there is information on the suspect's computer and that information might be resident on ISP, a TI warrant to access that.

With respect to wireless communications—and you are quite right that you do not need to be in the house at all; you can do that quite remotely—the bill envisages that we would need a TI warrant to do that under many circumstances. The analogy we draw with the execution warrant under section 3L is with a warrant on a post office box. If I send a letter to a particular person—for example, to John Smith at a particular post office box—my anticipation and belief is that it has arrived at the intended recipient's address when it is resident in that post office box. Nobody else has access to that post office box—in fact, people often have a key to get into it. You could draw an analogy between that and post that is sent to 'JohndotSmith' at an ISP account. The AFP's position is that, once that information has arrived at the ISP, the intended recipient then needs a key, usually a password, which can be entered into a computer from his home or anywhere around the world to give that person access to the ISP account. He or she unlocks that account and simply asks, 'What information do you have there for me to see?' It is no different from physically going into a post office box, turning the key and extracting your mail. The AFP's position there, of course, is that everything that flows after that is inconsequential for the purposes of the TI act.

**Senator LUDWIG**—I can access my Outlook, Word-based email and Internet when I am not at home or at my office.

**Mr Lammers**—Yes, you can access it from anywhere.

**Senator LUDWIG**—I can access it at the Qantas Club or wherever I can find a telephone line or a wireless connection.

**Mr Lammers**—Yes.

**CHAIR**—I can access mine remotely.

**Senator LUDWIG**—You need a telecommunications line and a computer—not a particularly sophisticated one, sometimes, either. You say that web based email is in the same category as that?

**Mr Lammers**—Yes.

**Senator LUDWIG**—In relation to mobile telephones, you say that the scenario that was related to Electronic Frontiers, where the machine is off and is then switched on, does not matter either—you can turn the machine on after executing a search warrant and collect the messages?

**Mr Lammers**—The current law allows people with a valid search warrant to access communication devices within the premises upon which we execute search warrants, including a scenario where a mobile phone is in the possession of a suspect. It is normal police practice not to allow a suspect to answer a mobile phone or even turn on a mobile phone or any other equipment. There are very good reasons for that, because we could lose evidence. If there is a mobile phone in the possession of a person in premises that we are searching and the mobile phone is switched on by police, for instance, and they see that there is a message, there could be two categories of message: an SMS, which is sent directly to the mobile phone and lives within the SIM card of the mobile phone, or a message that simply says, ‘Dial 101 and collect your messages.’ If we ask the owner of the mobile phone to turn on the mobile phone, then he or she may do certain things—and I guess this goes to operational methodologies now—which we would not want that person to do.

**Senator LUDWIG**—I thank you for your answer, but I was just trying to establish whether you now require a TI warrant to turn on a mobile phone and collect both SMS and 101 voice mail messages or whether that is part of what is available under a search warrant under 3L.

**Federal Agent Lawler**—Where a 3L search warrant is in play, the advice from the Commonwealth DPP is that it is lawful to do so currently. Where it is not under the provisions of 3L but under another head of power, where a search of a person is available under the law, then the advice from the Commonwealth DPP is that we are not precluded from doing so.

**Senator LUDWIG**—And you say that this bill will preclude you from both those actions that I just raised, including Web based email, SMS and 101 voice mail and personally scanning or opening emails prior to the recipient obtaining them.

**Federal Agent Lawler**—Yes. Furthermore, I think Federal Agent Phelan could give some very stark examples, in camera, of where that occurs quite regularly in an operational context and what the ramifications of that might be.

**Senator LUDWIG**—Also, the committee has just authorised a response from the Attorney—

**CHAIR**—They will not have seen that.

**Senator LUDWIG**—You will not have seen it yet, but I was going to ask you to have a look at it and then provide a comment to the committee in relation to these issues. They respond to some of your concerns, and I would like you to have a look at the response in the light of the evidence today and give us your view about that.

**Federal Agent Lawler**—We would be very happy to do that.

**Senator LUDWIG**—Thank you.

**CHAIR**—Thank you very much. Federal Agent Lawler, I am acutely aware that you have a personal time frame issue this morning as well.

**Federal Agent Lawler**—I do. It is in relation to the national security exercise that is running at the moment.

**CHAIR**—I understand absolutely. I doubt they will need us! In your submission on page 7, at points 29 and 30, you make some observations about vulnerability to viruses, spam and improper content and about the structure of the bill possibly making it difficult for the AFP to do their work in this area. I think the point that Ms Graham made, and I am not sure whether you were in the room at the time, was that there is an issue about the limits of a telecommunications system—that is, between the ISP and a private network—and about where that actually comes into play. If any of you were in the room at that time, do you have a comment to make on that?

**Mr Ryles**—Yes. In fact I would agree that there is a lack of clarity as to when a communication leaves a public network and enters a private network.

**CHAIR**—So, legislatively, we are in an area of ambiguity here.

**Mr Ryles**—Yes.

**CHAIR**—Is there a way to fix that?

**Mr Ryles**—As was mentioned in the opening statement, the UK regulations have actually addressed those issues and recognised that the owners of private communications networks should be allowed to do certain acts, such as open and view, in the course of that business to protect their own systems and business operations.

**CHAIR**—It may be, Federal Agent Lawler, that the committee decide to take up with the AFP and perhaps with Federal Agent Phelan some of those matters on a confidential basis if we need to following the conclusion of the hearing, but I do not want to detain you beyond the point that you said you needed to go. We will conclude with questions now in view of that but we may come back to you with some matters on notice. Obviously, if the information pertained to the matters you raised that Federal Agent Phelan was able to assist us with, we would receive that on a confidential basis.

**Federal Agent Lawler**—Thank you.

**CHAIR**—Thank you, Federal Agent Lawler, and your colleagues for assisting the committee today, and also for your submission, which raised some very interesting questions for our consideration.

[10.41 a.m.]

**HOLLAND, Mr Keith Colin, Assistant Secretary, Security Law Branch, Attorney-General's Department**

**SMITH, Ms Catherine Lucy, Principal Legal Officer, Attorney-General's Department**

**TEARNE, Ms Anna, Principal Legal Officer, Security Law Branch, Attorney-General's Department**

**WOODLEY, Mr Stuart Robert, Senior Legal Officer, Attorney-General's Department**

**CHAIR**—The committee welcome representatives from the Commonwealth Attorney-General's Department. The Attorney-General's Department has lodged two submissions with the committee, which we have numbered 6 and 6A. Do you wish to make any alterations or amendments to those submissions?

**Mr Holland**—No.

**CHAIR**—Mr Holland, would you like to make a brief opening statement before we go to questions?

**Mr Holland**—Thank you. I would just like to say a few words about the amendments intended to clarify the application of the act to modern telecommunications services such as email and SMS, in which there is a delay between dispatch of the communication by the sender and receipt of the communication by the intended recipient. We refer to these services as 'delayed access message services', as we have heard mentioned this morning already.

I am aware of reports suggesting that the bill will give greater powers to ASIO and law enforcement agencies to intercept email and SMS communications. Those reports are incorrect in that they mis-state the effect of the amendments. Rather, the amendments clarify when those communications continue to be protected by the Telecommunications (Interception) Act and when they will cease to be protected by virtue of becoming data rather than communications in transit. For some time we have recognised the need to clarify the application of the act to delayed access message services. The reason for this is that the act is built around the core concept of a communication passing over a telecommunications system. There are, however, some challenges involved in applying this core concept to delayed access message services, which may involve individual communications being stored at one or more points in transmission for varying periods of time.

The transmission of an email message, which we have heard so much about this morning, is an example of this. Depending on system architecture and other network factors, an email may be stored at the sender's mail server, the recipient's mail server and any number of additional points during its transit between sender and recipient. The challenge is to determine whether a communication stored in this way has ceased to pass over a telecommunications system or whether its passage over a telecommunications system has merely paused temporarily. Communications passing over a telecommunications system may not be accessed without the knowledge of the person making the communication other than in accordance with the act, usually under a warrant. Access to communications that are not or are no longer passing over a telecommunications system may be regulated by other laws, including laws governing the issue and execution of search warrants.

In 2002 the government introduced the Telecommunications Interception Legislation Amendment Bill, which included measures intended to clarify the application of the act to delayed access message services. Those measures were considered by this committee, which expressed some reservations about reductions in privacy protection and ambiguity in relation to whether a telecommunications interception warrant or a search warrant would be required to access communications stored at the premises of an Internet service provider.

We have taken the committee's comments on board in developing the amendments now before the parliament. In particular, the amendments now proposed ensure that a telecommunications interception warrant is required to access email stored at the premises of an Internet service provider that has not yet been accessed by the intended recipient. The revised approach also specifically excludes voice over Internet protocol services from the definition of delayed access message service. This very specific exclusion ensures that voice over IP services are not treated as delayed access message services merely by virtue of the negligible delay that may occur in the delivery of those communications. The exclusion does not mean that voice travelling over Internet protocol is not protected by the act; on the contrary, it explicitly ensures that voice over IP services receive analogous protections to standard voice telephony services.

In concluding, I emphasise that the interception act applies to all forms of telecommunications, extending *prima facie* protection to communications passing over the telecommunications system, whatever their form. The amendments now before the committee do not seek to erode that protection or to extend interception powers beyond those currently available. It might assist the committee if I ask Ms Tearne to address a couple of the issues that arose in the course of earlier evidence.

**CHAIR**—I suspect that that might be covered by questions, so why don't we hold off for a second. There are a couple of process issues we need to go through. I think you said at the beginning, and certainly the material for the bill says, that the legislation is intended to clarify the situation. But, with enormous respect, it seems in the light of the submissions which have been received by the committee from a vast range of players, both law enforcement agencies and groups like our first witness this morning, that clarity is hardly what we have achieved.

**Mr Holland**—With respect to some of those issues that were raised, I do not deny that in some areas that is absolutely correct. No-one would say that this area is crystal clear in every respect. That is why, as you would be well aware, this committee so frequently sees us before you—

**CHAIR**—We are always happy to do that.

**Mr Holland**—as we try to deal with what we thought when it was first developed was technology neutral legislation. Having said that, I also think some misconceptions have come up in the course of the submissions that have been put to the committee, and certainly some misconceptions about what it is that the bill proposes to do. It is the case that right now law enforcement can access emails. That is not at issue here. The question that is at issue is whether they access those emails via a search warrant or via an interception warrant. In the department's view there has been no doubt in advice that we have given in relation to the current legislation that, if you wished to access email stored at an ISP, then you needed a TI

warrant. We have given that advice. It is advice that has been supported by an opinion earlier on of the Solicitor-General.

It has only been with the advent of later legislation that the question has again arisen of whether or not general legislation relating to cybercrime overrides the specific legislation dealing with telecommunications interception. Again, the department has had very firm views on that and it has expressed those views on a number of occasions, both bilaterally and multilaterally, and in particular within the Interception Consultative Committee which all intercepting agencies have access to. It has been clear for two years that this issue was one that the government was going to deal with, and we have been discussing during the course of those two years how we might deal with it.

**CHAIR**—The legislation was introduced into the House on 19 February. We have the Australian Federal Police saying that there was not enough time to consult with them so that the concerns they have raised in their submissions could be addressed, but we all know that the process has taken at least two years. The New South Wales Police have come to us agreeing with some of the issues raised by the AFP. I go back to the question of what clarity we have achieved.

**Mr Holland**—The reason we do not have clarity in the one area that has been discussed, namely 3L, is that we—the department administering the legislation—take the view that the current legislation is clear on this issue but the DPP has taken a different view. In light of that, we have asked the AFP to provide us with all the material that they have that has led the DPP to form this conclusion, and we have sought the opinion of the Solicitor-General on this. That opinion has not yet arrived.

**CHAIR**—Because it has taken the Solicitor-General two years to come to a view?

**Mr Holland**—No, not at all. The Solicitor-General formed his view some time ago on what we had been saying. What we are talking about now is his second opinion. We are talking about section 3L under the Crimes Act that the AFP refer to. We as a department have been saying that our view is that that amendment, that particular provision, does not override what the law currently is. That is our view.

**CHAIR**—When did that 3L issue under the Crimes Act come to light?

**Ms Tearne**—I would have to check the date that the argument was first raised with us by the AFP and the DPP. It was raised some time ago—possibly over 12 months ago—and in that time the department indicated its own view that it did not share the reasoning advanced by the DPP in relation to its application of section 3L to the telecommunications interception regime. That issue has re-arisen in the context of consultations with the AFP and other interested parties on the current amendments to this bill. The AFP and the DPP again raised the question of the application of 3L, which the department had already indicated that it did not share. It is in the context of the reconsideration of that issue that the department sought a further clarifying opinion quite recently from the Solicitor-General.

**CHAIR**—How recently?

**Ms Tearne**—Before the introduction of the amendments, I could not specify the exact date. Certainly that opinion is currently being finalised. We do not have the final views of the Solicitor-General at this time.

**CHAIR**—You see the position the committee finds itself in.

**Senator LUDWIG**—There is a different interpretation of 3L. You say the AFP have got it wrong in that they are using 3L to broaden the powers which would otherwise require telecommunications interception legislation, as I understand it. They say that they can use an ordinary search warrant to access either opened or unopened web based emails at a residence, on a hard drive, however expressed. They can then use a search warrant to enter an ISP in the same way to access a recipient's emails even though they have not been delivered, because once an email has hit the ISP, they say it has been delivered like a letter in a letterbox and therefore the recipient can access it. You disagree with that view and you say that the DPP and the AFP's interpretation of 3L is wrong. Is that right?

**Ms Tearne**—That is correct.

**Senator LUDWIG**—As a consequence of that, you then say that you sought the first opinion. Is that available to the committee?

**Mr Holland**—Sorry, the first opinion was not on that issue. The second opinion is now being prepared.

**Senator LUDWIG**—When was that requested?

**Ms Tearne**—Again, I could not specify the particular date, but it was before the current amendments were introduced into the House of Representatives. I think it was around late January.

**Senator LUDWIG**—So the purpose of the current bill then was to clarify 3L as well?

**Mr Holland**—The purpose of this bill was to simply state what we understood to be the position and to put that beyond doubt.

**Senator LUDWIG**—But you are still waiting for a further opinion from the Solicitor-General to tell you that you have got it right.

**Mr Holland**—No.

**Senator LUDWIG**—Why would you seek another opinion if you say you have got it right?

**Ms Tearne**—The further opinion has been sought given that, obviously, this is a very important issue to law enforcement agencies and it is also a very important issue in the context of the community being able to tell at what point its communications are able to be accessed by law enforcement and at what point they are protected. In the development of these amendments we certainly considered, and we remain of the view, that the amendments in the bill do in fact clarify what is currently the legal position in relation to whether an interception warrant or a search warrant is required. However, during consultations on the bill, the AFP and the DPP made it clear that they maintained a contrary view to that that the department have been advancing. Having regard for the significance of the issue, we have sought a further opinion from the Solicitor-General. Unfortunately, he has not been in a

position to finalise that for us. However, he has given some consideration to the matter. If it assists the committee, I can say that he has indicated that his initial views are broadly consistent with those of the department on this particular issue.

**Senator LUDWIG**—So we have an agency that is using what could be considered expansive powers under 3L to access emails through search warrants that the Attorney-General disagrees with?

**Ms Tearne**—That is correct.

**Senator LUDWIG**—And your response to that is this bill. So it is not a development of the 2002 argument—you are still consulting on that.

**Mr Holland**—You are right. It is to put this beyond doubt. Clearly, when the AFP are acting operationally, their first port of call is to go to the DPP and seek advice as to whether or not they can do what they are doing. While we had taken a particular view on this, it was an issue that was clearly in dispute—as to what the impact of 3L was on the legislation. The issue itself had been of concern, as you know, from 2002. The difference between now and then, apart from how we are approaching it, is the fact that there has been this intervening legislative action which has been interpreted as having an impact upon the current legislation. So the government has decided to clarify precisely what the position is. It had been our hope and expectation that the Solicitor-General would have been able to give his opinion prior to this stage, but circumstances have prevented that. We would hope that, in settling this issue, we would not have the difficulties that have arisen so far.

**Senator LUDWIG**—Are we going to get a lecture on generalia specialibus non derogant? Is that what we are going to get?

**Mr Holland**—No, I am not going there.

**Senator LUDWIG**—It appears to me that you have an interagency dispute about the operation of current legislation that has not been resolved as yet and you are asking us to consider the amendments, which are designed in part to address the ongoing issue of telecommunications interception warrants—when they are required—and also in part to address the interagency dispute about the operation of legislation.

**Mr Holland**—No. With respect—

**Senator LUDWIG**—I am just trying to clarify where we are at.

**Mr Holland**—It is always difficult for us in this role as the administrator of the legislation because, as you have seen here today, Electronic Frontiers Australia, on the one hand, would take one view—

**Senator LUDWIG**—I think we got their view.

**Mr Holland**—and law enforcement agencies would take another. As the administrators of the act we have to look at the underlying purpose of the legislation, which is to protect communications travelling over a telecommunications system. That is the function of this legislation; that is the intention of this legislation. The difficult question that arises is: when does a communication actually cease its travelling over the system? We have said in these amendments, in working out the answer to that question, that in circumstances where 7(a) and

7(b) apply it is not then travelling over the system. So, if I have already accessed my email, law enforcement agencies can access that email stored on an ISP by virtue of a search warrant. That is what the legislation does.

**Senator LUDWIG**—How can they tell? For argument's sake, let us use the example I used earlier where I always have broadband on and Outlook running. The emails are turning up on my system all the time and I use a preview pane under Outlook, so I could effectively read the content of the email unless there is an executable file in there or something else which I then have to click on and open. The system does that when I am both there and not there, so I can preview it without actually opening it. If the AFP execute a search warrant on the ISP, can they view the emails that are unopened on my computer and can the ISP tell whether they are opened or unopened?

**Ms Tearne**—There are a couple of different questions there.

**Senator LUDWIG**—I am happy for you to take it on notice but if you could provide some clarity as to your position and run through it with us it would be useful.

**Ms Tearne**—I can provide a few comments on a couple of the issues that you have raised. There is certainly a question as to the means by which a law enforcement agency might determine whether a communication has already been accessed by the recipient. How that question is resolved would obviously depend on the means by which they seek to access that communication. If they are going to an ISP, for example, an ISP holds access logs that would indicate when a person has used their account and is therefore aware of and has downloaded the messages that are there for them. In circumstances of a search warrant and entry onto the premises, obviously the police would be conscious of the time at which they have entered the premises and there will also be indicators on the system of which communications have and have not been accessed. Certainly, there may be occasions on which it is not possible to determine conclusively whether or not communication has been accessed. Obviously, in those circumstances, the police will need to be able to point to or identify indicators that will demonstrate to them whether or not a communication has been accessed. Obviously access to communications that have not been accessed by the recipient attaches the higher threshold of an interception warrant and, in cases of doubt, that higher threshold would prevail.

**Senator LUDWIG**—The ISP will keep a log of whether I have accessed my email, how many have come through and come onto my system. I am running it all the time. It will show that I have received 30- or 40-odd emails while we have been sitting here. It will not show whether or not I have opened them though, will it?

**Ms Tearne**—No.

**Senator LUDWIG**—So the AFP execute a search warrant on the ISP and look at how many messages I have. It is 40-odd and they ask to look at them. As the ISP, you show them because they have issued a search warrant and, as far as you are aware, you are required to show them. When does the AFP decide that they really need a telecommunications interception warrant, or do they only find that out in a courtroom when someone asks them the sixty-four dollar question, 'Were they opened or unopened and could you tell'?

**Ms Tearne**—Certainly the amendments seek to set out a set of principles that will assist in determining when a telecommunications interception warrant is required and when those

messages have ceased their passage over the telecommunications system and can be accessed in a different way. The amendments do so by setting out a range of circumstances that describe how law enforcement go about that access and make quite clear that if access is effected in that particular manner then those communications are not in passage over the telecommunications system. That provides guidance that if you are accessing those communications in this particular way then they are not in passage over the telecommunications system and you have clear guidance that a search warrant is appropriate in those circumstances.

**Senator LUDWIG**—But if they cannot tell, what do they do?

**Ms Tearne**—Certainly there is also provision—

**Senator LUDWIG**—No, if they cannot tell. They have accessed a search warrant on an ISP, the log shows that I have got 40 emails and they want to read them.

**Mr Holland**—If in doubt, TL.

**Senator LUDWIG**—What if they do not?

**CHAIR**—How can we see that from the bill?

**Senator LUDWIG**—Yes. The AFP will assume that they accessed the messages. Some have been opened and some have not. The critical one is unopened. It then ends up in court. The person could be convicted without anyone ever asking the sixty-four dollar question. That is right, isn't it? If no-one asks whether or not it was opened, the person denies having received it and the log says they received it, it stops at that point. They do not ask the next question. The barrister might be in trouble for negligence, but I suspect Giannavelli and Wraith might save him. It seems entirely unsatisfactory that on the whim of an opened or unopened email a person can be convicted. I am happy for you to tell me that I am wrong.

**Ms Tearne**—Certainly the question as to the means in which communications are accessed and the matters that law enforcement agencies turn their minds to is one of the very significant things determining the test that does apply. There are already questions, and certainly there have been some raised this morning, about the scope of the application of the interception act and there has been some suggestion that the scope of the act is not clear. The department certainly takes the view that there are already some very clear principles on when communications are in passage over the telecommunications system and are therefore protected and thus law enforcement should be on notice to obtain the appropriate form of warrant.

As it stands, the interception act already makes it very clear that, *prima facie*, all communications passing over the telecommunications system are protected. That protection extends for so long as those communications are indeed passing over the system. The question that obviously arises, and which these amendments seek to address, is: when has the communication ceased its passage over the telecommunications system? The position in the department's view, which is supported by an earlier independent opinion on the matter, is that communications that have been downloaded onto the intended recipient's computer have, at that point, ceased their passage over the telecommunications system. Communications that are remotely stored, and in this context there is a distinction—

**Senator LUDWIG**—Like a web based email.

**Ms Tearne**—That is right—web based email and voice mail are remotely stored, and there are some other examples. Those communications cease their passage over the telecommunications system when they are retrieved by the intended recipient. Those are principles that already exist—they are ones that have been made known to law enforcement agencies quite widely. These amendments seek to put that matter on the face of the legislation so that it is abundantly clear to all who seek to examine the legislation.

**Senator LUDWIG**—I am sure you were here during the earlier evidence and heard the AFP speak. So, in your view, when the AFP—on executing a search warrant on a residence, for example—turn on a mobile phone, they cannot access 101, the voice mail, without a telecommunications interception warrant?

**Ms Tearne**—No, they cannot.

**Senator LUDWIG**—That differs from the AFP's view currently—and that is even before this bill.

**Ms Tearne**—That is right.

**Senator LUDWIG**—And you say that this bill will clarify that to the extent that they will require a TI warrant in respect of a 101 voice mail. But in respect of an SMS message, the act of turning on the phone will then download the messages to the SIM card within the handset. Do you say that that does or does not require a telecommunications interception warrant? What will the new bill do?

**Ms Tearne**—Certainly, in the department's view, the new bill does not do anything that the current interception regime does not do. So the law as it currently is and the law as it would be in the event that these amendments were passed is the same.

**Senator LUDWIG**—So it remains unchanged.

**Ms Tearne**—In terms of the issue you have raised about voice mail communications and SMS, there is certainly a distinction there in that the SMS communications are ones that are downloaded to a particular piece of equipment, the SIM card, in the handset. The voice mail communications are ones that are remotely stored by the provider of that particular service. Certainly SMS communications that are present on a handset that is in the lawful possession of a law enforcement agency—for example, under a search warrant—are ones that have ceased their passage over the telecommunications system to the extent that they have been downloaded to a particular piece of equipment.

**Senator LUDWIG**—Notwithstanding who initiated the download?

**Ms Tearne**—That is correct. In the context of SMS messages, SMS messages are pushed down by the service provider—

**Senator LUDWIG**—Yes.

**Ms Tearne**—They are not actually requested by the user and so they will appear on our phones when we are not with them. They will arrive and then be downloaded.

**Senator LUDWIG**—So even if the person has not read them?

**Ms Tearne**—That is correct, they are downloaded and the person will read them later.

**Senator LUDWIG**—So you only require a search warrant for that?

**Ms Tearne**—Yes.

**Senator LUDWIG**—Sorry, did I interrupt you? Was there something more you were going to say?

**Ms Tearne**—I was going to add some additional comments on the voice mail issue. That situation is somewhat distinct in that those voice mail messages are remotely stored with the service provider, and remote storage at a point in transit—so before it has reached the intended recipient by the intended recipient retrieving those communications—continues to pass over the telecommunications system. They are therefore protected by the prima facie prohibition against interception, and access to a voice mail message stored with a mobile service provider is one that would require an interception warrant where that message has not yet been retrieved.

**Senator LUDWIG**—And that is your position now and with the new amendment?

**Ms Tearne**—That is correct.

**Senator LUDWIG**—That differs from the AFP's view.

**Ms Tearne**—Yes.

**Senator LUDWIG**—They say that they can access the telecommunications provider and access the voice mail with a search warrant and that they can access the 101 voice mail with an ordinary search warrant—or, if they have apprehended a person or a suspect in the street then they can remove the phone, turn it on and access the 101 voice mail in the usual course of operation.

**Ms Tearne**—That is correct. My understanding of the AFP's position is that under a search warrant they have the authority to operate certain pieces of equipment, which would include a home computer. The AFP consider that that access allows them to access anything which they could retrieve remotely. However, the department takes the view—and we have received preliminary confirmation that this is indeed correct—that the general provisions of a search warrant do not have the effect of overriding the very specific protections that are conferred upon communications that remain in transit. While a communication is at an intermediate point in its transition between sender and recipient, it continues to be protected and it cannot be accessed under a search warrant.

**Senator LUDWIG**—And that would include a mobile telephone on a person when, say, there has been no execution of a warrant but they are suspected of an issue, they have been apprehended perhaps and the mobile phone has been removed from their possession. You say that the AFP cannot access the 101 voice mail.

**Ms Tearne**—That is correct.

**Senator LUDWIG**—And you say that screening for viruses, trojans and all such manner is permissible currently and under the amendment in the new bill. Is that right?

**Ms Tearne**—Yes.

**Senator LUDWIG**—Does that also include what the AFP went to when they said that they have security personnel who open an email, check its content for inappropriate material, close it again and then forward it to the recipient to see what happens in some instances? It seems to be an integrity measure they put in place. They also check whether there is a virus, parasite or trojan. They use their internal security people who are familiar with electronic devices to ensure that they are not only machine processed but visually processed, if we can call it that, or read.

**Ms Tearne**—No. The department's view does not go quite so far as the proposition you have outlined and that the AFP outlined previously. The issue that the AFP has raised goes to a different part of the amendments—that is, the extension of the prohibition against interception to include reading or viewing of a communication. At the moment, that prohibition is limited to listening to or recording a communication. While the concept of recording is one that translates into the electronic communications environment, listening obviously does not have such an easy application to text and imaged based communications.

The extension of the prohibition against interception to reading though is not one that in the department's view has the effect of precluding electronic content filtering of email communications. The meaning of 'reading' extends only to reading in its human intelligible form in the sense of apprehending the content of a message and comprehending that. It does not extend to electronic filtering mechanisms, so content filtering devices that are commonly used in both government departments and private places of business to ascertain the technical characteristics of an email communication—for example, software scanning to identify file extensions that may contain malicious code viruses et cetera or even to scan for particular combinations of malicious code—will not be precluded by the amendments. So if the amendments were passed, the AFP would still be able to use content filtering to ensure that both malicious code in the form of viruses, trojans et cetera and also inappropriate content in the form of picture extensions and the like do not penetrate their information technology systems.

**Senator LUDWIG**—But they could not use what they currently do as their integrity measures and physically open emails, check the content and then sometimes close them and let them go to see what happens?

**Ms Tearne**—No, that is correct. They could not. Any circumstance in which a record of a communication is created prior to its being received by the recipient and reaching the end piece of equipment amounts to an interception under the current law. The amendments extend the definition of 'interception' to preclude viewing, so that would indeed preclude viewing of communications before they reach the end user.

**Senator LUDWIG**—So every time their email server picks up a suspect email that they thought might contain a trojan, a parasite or some other virus, or alternatively might contain inappropriate content, their security personnel cannot check that by opening it?

**Ms Tearne**—That is correct.

**Senator LUDWIG**—That would require a telecommunications interception warrant. Have you asked the AFP how many instances that would be?

**Mr Holland**—No.

**Senator LUDWIG**—You must have asked the AFP about this issue before. You must have consulted about it, surely.

**Mr Holland**—It came up in the discussions that we had in January, when we were talking about the bill then. This issue was raised at that stage. The processes that Ms Tearne is talking about are already available and have been used in the context of the department. For example, in the four years that we have been using those—and we have 15,000 ingoing and outgoing emails a day—no virus has been through the system.

**Senator LUDWIG**—I have one on mine at the moment.

**Mr Holland**—In our case, we just get a note saying: ‘This message has arrived. It’s been blocked. It will not be let through unless you tell us its work related. We blocked it because it may contain offensive material or a virus.’ So we are notified but so too is the person who sent the email. They are also told. We have been doing this for four years. It is not as though the threat of trojans, viruses or whatever is not real, but all we can say is that, in our case, in the four years we have been using these systems they have not got through.

**Senator LUDWIG**—Have you consulted with the AFP on this issue, because it appears that you have not been able to convince them? Have you consulted with them about their particular concern being unfounded?

**Ms Tearne**—We have certainly indicated the position that is outlined in our supplementary submission—that is, the department consider that the extension to reading will not preclude them from using electronic content filtering. We have not had the opportunity to discuss the example that Keith has just outlined in terms of our department’s own measures which have, to our understanding, been very effective in both ensuring the protection of our information systems and preventing the entry of inappropriate content. Certainly the issue of whether the extension to reading would preclude electronic scanning is one on which we have made our views to the AFP clear.

**CHAIR**—But they are not talking about electronic scanning.

**Senator LUDWIG**—No, and neither am I.

**Ms Tearne**—No. As I said to Senator Ludwig earlier, the AFP do take an extra step and have indicated their view that physical intervention on the part of an IT security officer is something that is necessary to maintain the integrity of their systems. In the Attorney-General’s Department we do not employ a person to view a communication before it gets to a recipient. We use exclusively electronic content filtering and scanning mechanisms. To that extent—the use of that mechanism—we have found that to be a protection.

**CHAIR**—We understand all of that, but the point is that the AFP has a different system. Your supplementary submission does not go to the point that the AFP makes. In fact, your supplementary submission manages to go for a page and half to the submission of Privacy Victoria and for two paragraphs on the Australian Federal Police, the operational organisation charged with implementing the legislation. We do not have an answer from the Attorney-General’s Department on the issues raised in the Australian Federal Police’s submission.

**Senator LUDWIG**—And we doubt whether you have even consulted with them about it.

**Mr Holland**—We tried as quickly as we could in the time frame to get back to the committee on those submissions. Clearly there are other matters that we will have to come back to the committee on.

**CHAIR**—Mr Holland, the committee are the beneficiary of a timetable from the Senate that has us reporting on this bill on the 30th of this month. We are the beneficiary of a range of submissions which leave the committee in some doubt as to clarity being achieved. We would really appreciate your assistance and cooperation. We do appreciate the supplementary submission. I did not mean to imply that we do not, but it does leave in my view—and I think in the view of other committee members—a number of outstanding issues. I will go to the amendments relating to the Australian Security Intelligence Organisation. What evidence should the committee be turning their mind to, to understand why these amendments are necessary?

**Ms Tearne**—There are two amendments in relation to the Australian Security Intelligence Organisation. Are you referring to both of those or to one in particular?

**CHAIR**—To both.

**Ms Tearne**—I will take them in order. Firstly, there is the amendment to allow ASIO to record calls to its publicly listed numbers and to do so by way of an exception to the prohibition against interception. That particular amendment is designed to address an operational consideration on the part of the organisation. The publicly listed numbers for the organisation are the ones that are used by members of the public to contact ASIO and to advise it of matters that may be of security interest. The organisation takes the view that it is very important that there be an accurate recording of those communications in the event that those numbers are used to pass on security relevant information and also to record any threats that might be made via those numbers.

**CHAIR**—Why is it too hard to tell the caller that the call is being recorded?

**Ms Tearne**—Certainly it is possible to tell the caller that a call is being recorded, and that would take it outside the realm of the interception. However, there are two issues in that regard. The first is that a verbal notification to a caller obviously represents a delay in the communication and, to the extent that absolutely time-critical information is being imparted, the delay that is created by providing that notification could represent one that has significant consequences in terms of a time-critical situation. The other side of that issue is that, certainly, a notification to the caller that their communication is being recorded may in some cases represent a deterrent to callers passing on information that is very important to the organisation and important to the performance of its functions.

**Mr Holland**—That first argument, Chair, was actually the justification for a similar provision relating to 000 calls.

**CHAIR**—Yes, and we know what happens with those. And the second one, Ms Tearne?

**Ms Tearne**—The second amendment removes the requirement to notify a carrier in certain specific circumstances. Under the operation of the telecommunications interception regime as it currently stands, there is a requirement to notify a carrier when interception is being effected with the assistance of that carrier. However, there are circumstances in which the

organisation may seek to effect that interception without reference to a carrier. That may be because of a particular emergency, a particular critical situation in which it is more appropriate to deploy an alternative form.

**CHAIR**—More appropriate to do what, Ms Tearne?

**Ms Tearne**—It may be more appropriate that the organisation effect the interception itself.

**CHAIR**—ASIO?

**Ms Tearne**—Yes, as opposed to the carrier.

**CHAIR**—And to deploy an alternative what?

**Ms Tearne**—To deploy alternative measures, to do something otherwise than in accordance with the standard procedures. The other situation in which this could potentially be an issue is in circumstances where approaching a particular carrier may prejudice either a particular investigation or security generally.

**CHAIR**—How has the consultation gone with industry on this? What does industry think about this amendment?

**Ms Tearne**—I am not aware of the views of industry in relation to this particular amendment.

**CHAIR**—Is that because they have not been consulted?

**Ms Tearne**—That is correct.

**CHAIR**—Why not?

**Ms Tearne**—Because certainly this amendment affects the way that ASIO performs its particular functions and, where it was executing a warrant in this particular manner, that would not involve any interference or interaction with a carrier's own systems. This amendment is principally designed to ensure that security is not prejudiced by providing particular notification in circumstances where it is not necessary and there is no interactivity with the carrier in relation to that interception.

**CHAIR**—How can we guarantee no impact on anyone's systems?

**Ms Tearne**—In terms of interference with systems?

**CHAIR**—Yes. How do we guarantee no interference with the systems? I do not understand the technology.

**Ms Tearne**—I would not be in a position in a public forum to comment on the very specifics of that technology, unfortunately.

**CHAIR**—Should we go in camera? Would that help you?

**Ms Tearne**—I think the comment that I could offer is that the Australian Security Intelligence Organisation is obviously subject to some very significant oversight mechanisms. In circumstances where it was seeking to execute an interception, it would always need to do so in accordance with a telecommunications interception warrant and in accordance with the additional constraints that are already set out in the interception regime in relation to how it does that. That is the subject of legislative requirements in terms of what it does on

interception and it being lawfully authorised, and also, independently, the Inspector-General of Intelligence and Security obviously has oversight of the organisation's performance of its functions and how it does that in ensuring that that is done in a manner that is consistent with legislative constraints.

**CHAIR**—I understood that, in our implementation of counterterrorism measures and similar sorts of law enforcement initiatives that have been taken in recent times, we were at pains to work with industry in, for example, the protection of key pieces of infrastructure and the relationship between industry and law enforcement to ensure that Australia did this particularly well. I am confused as to why we would not have consulted industry, the telecommunications industry in this case, about the implementation of this particular amendment.

**Ms Tearne**—I certainly did not mean to suggest that there was not a good relationship with industry in the interception context. We have very long-established relationships with a range of service providers in the context of telecommunications interception.

**CHAIR**—I understand that.

**Ms Tearne**—Although the specific providers were not directly consulted in the development of these particular amendments, having regard to the reasons I outlined previously about the way in which they would actually function, we certainly have not received any comments. I believe Optus has made a submission and has not raised any concerns, and we are not aware of any concerns that have been raised by industry through the day-to-day relationships that we have with them.

**CHAIR**—That is not really the point. It is not the role of this committee to do the consultation with industry before a bill is brought forward in this way, so your telling me that the committee has received a submission from Optus that says it is fine does not really answer my question about the extent of consultation from the department—or perhaps it does.

**Senator LUDWIG**—You might want to deal with this in a confidential submission or in camera. The submission goes to the issue of notifying the carrier, but they may not know which carrier. Would they know in each instance which carrier it is, depending on the device they use?

**Ms Tearne**—A particular telecommunications service is always provided by a carrier. In order for any law enforcement agency, or indeed ASIO, to obtain a telecommunications interception warrant it is first necessary to identify a service.

**Senator LUDWIG**—So they know which carrier they are using under the TI warrant—or can the TI warrant express a range of carriers?

**Ms Smith**—There are two types of warrants. One will identify the person who is subject to the warrant.

**Senator LUDWIG**—A named person warrant.

**Ms Smith**—That is correct. The other one will name the service.

**Senator LUDWIG**—A named person warrant does not necessarily identify the carrier, so there could be a range of carriers.

**Ms Smith**—That is correct, and in fact a telecommunications service warrant does not notify who the carrier is either. A particular named person warrant or telecommunications service warrant can actually be executed on a number of carriers. As we use our mobile phones they may roam from carrier to carrier depending on where we are travelling, so there is a need to serve it on more than one carrier in some circumstances. The name of the carrier is never notified on the face of the warrant itself.

**Senator LUDWIG**—What will this bill do in relation to both the named person warrant where the name of the carrier is not provided and the service warrant where you serve it on a number of carriers, because there might be eight or nine different mobile carriers and the suspect might be using eight or nine different SIM cards with eight or nine different carriers. What will this bill do in relation to those two instances? You might want to take it on notice if it will take longer than five minutes.

**Ms Smith**—I am happy to take it on notice. Briefly, though, in circumstances where there are eight or nine carriers which a warrant may need to be served upon or where for security purposes there are concerns about providing a copy of the warrant to the service provider because there may be some concern that that service provider is somehow linked with the target, this bill will allow the Australian Security Intelligence Organisation to protect the information that is on that warrant and not provide it to the carrier where they can intercept on another basis without physically giving them a copy of the warrant. I think I would need to make a confidential submission to provide more details on how that is done.

**Senator LUDWIG**—If you would not mind providing details on both of those two instances—

**CHAIR**—Which the committee will receive on a confidential basis.

**Senator LUDWIG**—Of course they may be using other means to access the communication outside the usual course of ways we might imagine. I think that is what you are alluding to, Ms Tearne. Is that right?

**Ms Tearne**—Yes. The effect of the amendments is to apply an exception—

**Senator LUDWIG**—It covers all those things as well.

**Ms Tearne**—That is right, yes.

**Senator LUDWIG**—In that instance they may not know the carrier they are borrowing from—or would they always know the carrier?

**Ms Smith**—As you said earlier, you can go anywhere to access your service and it may not be possible to go to a particular Internet service provider whose service we can guarantee you are utilising. It may be that your communication is bouncing through various providers so it is hard to track it down.

**Senator LUDWIG**—I can imagine how that could be done. You might want to deal with some of those issues in the confidential submission.

**CHAIR**—I do not think there are any further questions but, as we just agreed, there are some follow-up issues which the committee will, where it is appropriate, happily receive in the form of confidential responses. From this morning's hearing there will be some other

questions on which we would appreciate your further advice. Mr Holland, in terms of the advice the department is awaiting from the Solicitor-General—on the matter we were colloquially describing as 3L—we are used to the committee being told we cannot receive copies of the Solicitor-General’s advice. That is an issue for another time, usually, but if information that would assist us with our deliberations is made available before the committee is required to report to the Senate we would be grateful to receive it.

**Mr Holland**—Absolutely.

**CHAIR**—Thank you very much to the officers of the Attorney-General’s Department.

**Committee adjourned at 11.31 a.m.**