COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE

Reference: Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

THURSDAY, 1 JULY 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

SENATE

LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE

Thursday, 1 July 2004

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

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

Senator Bartlett for matters relating to the Immigration and Multicultural Affairs portfolio

Senators in attendance: Senators Ludwig and Payne

Terms of reference for the inquiry:

Telecommunications (Interception) Amendment (Stored Communications) Bill 2004.

Committee met at 9.03 a.m.

CHAIR—This hearing is in relation to the Senate Legal and Constitutional Legislation Committee's inquiry into the provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004. The inquiry was referred to the committee by the Senate on 16 June 2004 for report by 22 July 2004. The bill amends the Telecommunications (Interception) Act 1979 to change the way in which it applies to stored communications. The amendments will have the effect of limiting the prohibition against interception to the live or real-time interception of communications transiting a telecommunications system. The committee has received nine submissions for this inquiry, eight of which have been authorised for publication and are available on the committee's web site. One has been received as confidential. Witnesses are reminded of the notes they have received relating to parliamentary privilege and the protection of official witnesses. Further copies of those 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 session. It is important that witnesses give the committee notice if they intend to ask to give evidence in camera.

[9.05 a.m.]

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

CHAIR—Welcome. Electronic Frontiers has lodged a submission with the committee, which we have numbered No. 1. Do you wish to make any amendments or alterations to that submission?

Ms Graham—No.

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

Ms Graham—I will not repeat everything we have written in our submission. I am aware that the committee is on, as usual, a short time frame. I would like to stress a couple of points that I feel may be overlooked in the wealth of submissions and so forth that have been lodged. We are alarmed that some agencies are advising that this bill will not give them new or greater powers. We find that amazing because this bill unquestionably gives all police and other government agencies power to access undelivered communications that presently cannot be accessed without a telecommunications interception warrant. We also would like to stress that the bill is not only about giving additional powers to the Australian Federal Police. The same powers that are going to become available to the Australian Federal Police are going to be available to both criminal and civil enforcement agencies in the states and territories.

We also find the grounds that have been put forward for this bill—urgent operational needs—to be quite surprising. The term 'operational needs' seems to have first started becoming prominent just after February or March this year, and it originally seemed to arise because of the last bill extending the definition of 'interception' to reading and viewing. At that time, the AFP said that their existing processes for checking whether emails contained viruses and so forth already included copying communications in transit. They said that copying was fundamental to their process. We would like to note that copying communications in transit has been illegal probably for 25 years. If the AFP have been copying communications in transit and neither they nor the CDPP has prosecuted them yet, it seems very unlikely to us that they will be prosecuted in the near future. Therefore, it seems to us that the bill cannot be justified on the grounds of the AFP's internal processes and their wish to be able to copy emails. If they are doing it now, it seems unlikely they are going to be prosecuted while this bill is being reviewed.

The other matter is remote access using section 3L of the Crimes Act. EFA are very much of the view that that should not be permitted in relation to incoming communications because, amongst many other things, when the AFP are on warrant premises, the warrant that they are executing may not concern serious crimes or crimes that are specified in the Telecommunications (Interception) Act. This in effect means that, if they are able to use section 3L, they are able to access communications that they would not be able to access with a telecommunications interception warrant. The incoming messages that they would be accessing while searching through somebody's computer are not messages that are written by the suspect—they are messages written by anybody else who happens to be emailing the suspect at the time the police are searching the suspect's computer. We therefore consider that

there should be a very high threshold on the police being able to access incoming messages while they are on warrant premises searching through someone's computer, because it is not that person's own communications that they are accessing, it is the communications of other people, who may well be law-abiding citizens.

We would also like to note that on the matter of this remote access, where it has been said that if the police are not able to do this while they are on warrant premises they would have to go away and evidence could be destroyed and all of these matters, we noted during testimony given to this committee on the Surveillance Devices Bill that it apparently takes 20 minutes to get a telecommunications interception warrant over the phone. We therefore do not see any reason why, if the police go to warrant premises and determine that there may be emails that they wish to be able to download, they should not have to telephone a judge or a member of the AAT and obtain a telecommunications interception warrant to do so.

We are also concerned about claims that the AFP would have to turn computers off to stop the emails being downloaded. We would like to note that to the best of our knowledge all email packages can easily be configured not to automatically download messages. Therefore, if the police are on premises where the messages are being automatically downloaded, they can configure that email package to stop doing that. If the AFP do not know how to do that, the AFP are empowered under section 3L of the Crimes Act to guard or lock up that computer until they can get expert assistance to do whatever they need to do to be able to access information on that computer. So, once again, we do not see that this operational need in relation to remotely accessing communications that have not yet been delivered holds water, because the police already seem to have powers whereby they can get warrants, guard equipment so that it cannot be interfered with and so forth. In summary, what I am trying to express is that we do not see this bill as being in any way necessary at this point in time. It is certainly not urgent.

Senator LUDWIG—This has been a little bit of a trip, in the sense that it started with the amendment to the TI bill of 2002. You may also recall—you may have read the transcript—that Attorney-General's and the AFP seemed to be at odds over what power they had presently in relation to telecommunications interceptions warrants and whether they are required or whether an ordinary search warrant is required. What I am interested in at the moment is: if this bill is not passed, do they not have the power under 3L anyway to access a stored communication on an ISP without a telecommunications interception warrant? Is that your understanding?

Ms Graham—My understanding is that whether or not they have that power depends on whether you take the advice of the Commonwealth Director of Public Prosecutions or the advice of the Solicitor-General. The fact that the government now wish to pass this bill in order to make it clear that they have the power under 3L to access remote communications suggests to us that the Federal Police at present are not confident enough about their power to do that to be willing to obtain evidence in that way and risk it being thrown out in a court. We therefore consider that there are serious questions about whether the AFP would use section 3L and whether they have in fact been accessing using 3L. In all of the transcripts that I have read I cannot recall seeing the AFP having said anywhere that they do use section 3L. They say they have the power to use section 3L. I think it would be very interesting to know

whether they have actually been using it on the assumption that the evidence would not be thrown out in court.

Senator LUDWIG—Is Electronic Frontiers' current view about stored communication that there should be a telecommunications interception warrant for all communication stored by an ISP? Or do you think there are exceptions?

Ms Graham—Our overall principle is that we do not think that police, or any other government agency, should be able to access stored communications from, for example, an ISP where there are insufficient accountability and control mechanisms, because the individual does not have any idea that that is being done. The access is being done covertly. However, we also accept that once communications have been delivered to the recipient or have been accessed they are then stored communications—they are no longer being transmitted over the telecommunications system.

Under the bill that was put forward in February, we accepted that communications were protected until they had been opened or otherwise accessed et cetera. Once the material had been accessed by the intended recipient, the police would still be able to use a search warrant to access those communications at the ISP if the ISP had retained a copy. That was a matter that EFA raised in our submission with regard to backup copies and so forth. Our question was what kind of warrant was needed if ISPs had retained copies of people's communications without their consent—if they had copied them before the person had even received them. We felt that the bill needed to be amended to make that clear one way or another. Our overall view is that we do not think that police or any other agency should be able to access private communications on someone else's premises without either a telecommunications interception warrant or notice to the person whose communications it is. It is similar in the USA, for example. I think the Victorian Privacy Commissioner's submission either this time or last time referred to the rules under the US regime that apply if they do not want to get a higher standard warrant. They have to notify the person whose communications are being intercepted. This is a means of making sure that abuse is not occurring because of the wide-ranging powers under this bill to potentially access without a warrant. Certainly, under this bill there are some circumstances to access without a warrant at all.

I am trying to say that, in principle, they should need an interception warrant or give notice if they are going to access a service provider's premises. Whilst that is our preference, there is still a difference between messages that have been delivered and not delivered. That is why we would have accepted that bill in February, because at least it ensured that the messages could not be accessed without an interception warrant until the intended recipient at least knew the messages existed. So there are two levels. Our first priority is that they should not be accessible without a warrant. Our second one is that if that cannot be achieved, for whatever reason, then at the very least undelivered messages should require an interception warrant. Does that clarify our position or not? It is very complicated, as you know.

Senator LUDWIG—I can go back and read the transcript. It is helpful. Difficulties still remain in my mind with respect to SMS, where you pick up the handpiece and the SMS messages will then be received. The recipient may not be aware of the SMS messages, although you might glean from the content that they are. Equally, there are difficulties with accessing a computer where you have both delivered and undelivered messages. It is very

difficult to tell whether or not the recipient has accessed them or not because you can configure the computer differently. So it makes it difficult, I suspect, viewing a computer screen by a search warrant under a police investigation. If they can see delivered and undelivered messages, it makes it difficult not to view those that may be set up with preview window panes that are not read. It would be hard to distinguish between those messages and ones that have been opened but they do not know by whom—it may not have been by the person who owns the computer or is in the residence. It could have been someone else that had called in. I still do not understand quite how what you are putting works in that context, but I do not expect you to be able to summarise and answer now.

Ms Graham—I can possibly help. We have given a considerable amount of thought to that as things have developed over the last months. There certainly is this issue of whether a message on an individual's computer or mobile phone has been read or not. Certainly it will be difficult in some circumstances for the police to know that. My understanding was that the bill in February or March made clear that, once the person had opened or otherwise accessed the messages, access would be available with a search warrant or some other form of lawful authority. It is unfortunate that some people leave their computers on all day automatically downloading messages and that they have preview panes open and so forth.

The fact is that if people are concerned about the potential for their home to be raided and messages to be accessed, they can shut down their email client before they go out the door and have a password in the email client so that if someone opens the email client they will have to enter the password before it will start downloading messages. I think we might be at a point where we have to accept that people have to be responsible themselves for how they use the technology and the extent to which what is on their computer is made available to other people. My understanding is that the same applies to mobile phones if you leave your mobile phone in your home and somebody raids your home. I do not know about anybody else's mobile phone, but mine has a password on it. If someone raids my home and my mobile phone is there and they turn it on, they cannot access it without knowing the password. So they cannot download the messages.

I really think that the way that the law has to work is that the limitation on accessing messages that have not been delivered has to be along the lines of what was in the bill in February—once the person has read or otherwise accessed. One has to accept that, if a person has set their computer to automatically download messages from their service provider, that is accessing those messages, because the person has to configure their computer to do that.

Senator LUDWIG—Move one step back up then—from the ISP. At that point do you then say that a telecommunications interception warrant is required?

Ms Graham—I am sorry—at what point?

Senator LUDWIG—At the ISP of undelivered messages.

Ms Graham—Yes, that is right. My understanding is that an ISP will always be able to tell whether a computer down there has accessed the message.

Senator LUDWIG—That was my next question.

Ms Graham—They will know whether that message has been downloaded or not. I will also mention on that matter that there has been a great deal said about web mail. Web mail is no different from IMAP or POP mail. There are three—well, there are not necessarily even three—different protocols.

Senator LUDWIG—There are only two.

Ms Graham—The AFP in their submission earlier this year talked at length about POP and IMAP protocols for accessing email. My understanding is that web based email uses IMAP. There are some IMAP clients—mostly older software, I am told by ISPs—that will not identify whether a person has actually opened the message when they access it on the web. But they will identify that the headers of that message have been shown in a web page—that is, that the person has seen the subject lines and the 'from' fields. They might not have clicked on that message to actually read what is inside it, but they have seen it on a web page screen saying, 'Message No. 1 from so-and-so, subject line et cetera'. As I understand it—and I did make a lot of inquiries earlier this year—web based email uses IMAP and most probably all IMAP software will identify whether the person has seen the subject lines and the headers. We are 2½ years down the track since this whole matter was first raised in 2002. I do not mean new software; I just mean upgraded versions—software keeps getting upgraded constantly.

Senator LUDWIG—Unfortunately.

Ms Graham—My understanding is that current versions of IMAP software will not only identify whether the person has seen the subject line and the 'from' field—or whatever—on the webpage; the records that are back at the ISP's premises will also show whether the person actually clicked on the email and opened it. The ISPs can find this out because all of those emails that seem to be sitting in cyberspace on a webpage are in fact stored on the ISPs' servers in the same kind of place that any other email is. They can look in what is called the headers of the message and, if the subject lines and so forth have been viewed, there are numbers and things in the headers that mean that an ISP is able to tell whether or not it has been read. When people look at their emails, they do not see the headers of the emails. They see the 'to' and 'from' fields, the subject line and the date. Those are part of the headers.

There is also a considerable amount of other information that is in the headers that to see in most packages—like Outlook and so forth—you have to click another button or something to say, 'Show me all the headers; don't just show me these four.' On an ISP's system there is that information and, I understand, additional information—that is, where numbers, dates, times and things change between when the message was received on the system and the last time anything happened to it on the system, like if someone downloaded the headers so that they could see the subject line in the web client. Things in the headers that are stored on the ISP's system change.

I do not wish to give the committee the impression that I am saying that in every single instance ISPs are going to know this. What I am saying is that I am told that the newer versions of software make this markedly easier for ISPs to know and that I understand, even with the older software, that at least they were able to know whether the subject line and the 'from' field, for example, had been seen on a webpage. I may be mistaken about that, but I am told that technology has moved along in this. I would be extremely surprised if businesses like

Telstra and BigPond—all of those major ISPs—were not able to identify whether messages had at least been accessed by the subject lines being viewed on a computer screen.

Senator LUDWIG—You may not have seen it because of the short time frame involved, but the Australian Securities and Investments Commission mentioned in their submission that in their view—and I might have got this wrong, but as I understood it this was their view—emails are used by business a lot now, that they replace the general memorandum or letter and that, as such, emails are removed from their access. They would have otherwise been able to obtain memorandums or letters without TI warrants and the like and without the particular technologies and other warrants that now have to be put in place. Do you have a view about that? It means that emails are then treated differently from ordinary mail.

Ms Graham—They will also be treated differently from faxes.

Senator LUDWIG—Yes. You accept that? That is what I am trying to ascertain. You say that they should be?

Ms Graham—Yes. Our view is that, irrespective of what is attached to the email, the email is a communication, a telecommunication, and it should be subject to strict privacy rules. If ASIC does not feel it has sufficient powers at the moment to access whatever it is it needs to access then I think it is a matter for ASIC to convince the government and the parliament that it needs greater powers for specific reasons. Those specific reasons should be identified in the same way that serious crimes are identified in the Telecommunications (Interception) Act. The serious risk is this. Even if one says that perhaps in some circumstances ASIC should be able to do this or that, this bill is not just dealing with ASIC's perceived problems; it is granting a vast number of agencies increased powers. I would also like to mention that I understand that ASIC probably will not be happy with its powers until ISPs are required to log and record every single thing that an Internet user does on line.

Senator LUDWIG—I do not think their submission goes that far.

Ms Graham—Not in this instance, Senator. But, with respect, submissions by ASIC and AUSTRAC to the former Parliamentary Joint Committee on the National Crime Authority in 2001 did call for powers whereby either ASIC or AUSTRAC—this was reported in the committee's report as well as in *Hansard*—

Senator LUDWIG—I suppose it is important for ASIC to know which one, though.

Ms Graham—It probably is, but they are all part of the AGEC group.

Senator LUDWIG—I know that, but perhaps you could qualify an agency rather than choose one that might be not the one.

Ms Graham—Yes, I can let you know.

Senator LUDWIG—I am happy for you to take it on notice and let us know.

Ms Graham—I could certainly let you know.

Senator LUDWIG—It is drifting away from where we are now.

Ms Graham—Yes, it is just the issue of the whole Internet means of communication. Agencies are constantly saying they need more and more powers and they want the powers simply with a written notice. They want to be able to just go into an ISP with a written notice

and, for example, be able to take a copy of the entire hard drive of an ISP. So my relevance is that, even if one is going to say that ASIC should be able to access emails without an interception warrant, this is still not going to resolve the problems that ASIC or AUSTRAC believe they have in terms of being able to access information. The powers will go on. It will keep going on with what is required. We are saying that the line is drawn where it is now and the line should stay drawn where it is now.

Senator LUDWIG—I have one last question. Do you think this bill, if it were to pass, would give the ISP the ability to read customer emails?

Ms Graham—Absolutely. The bill itself and the explanatory memorandum makes quite clear that the restrictions that exist at the moment on the circumstances on which ISPs would be able to trawl through people's email would cease. It would no longer be an illegal interception.

Senator LUDWIG—I guess that might have been the penultimate question. This is the last question I have. The Attorney-General's Department have indicated that there should be a 12-month period for this legislation to operate within whilst a review is being conducted. Do you have a view of that and about what the terms of reference of that review might be?

Ms Graham—A view about the actual review?

Senator LUDWIG—Yes.

Ms Graham—We certainly think that the review is necessary. There are certainly a number of aspects of the interception act that in our view could well do with review and clarification and all of those kinds of things. It is a concern that at the moment there seems to be no indication as to whether this will be a public review, whether submissions will be called for, whether the results of the review will be made public. Basically, we feel that such a review should take place in a way similar to a committee inquiry. We note, for example, that the Attorney-General's Department issued an exposure draft for a telecommunications offences crime bill a couple of months ago. That was put out for public consultation first. We really do think that any review of the Telecommunications (Interception) Act should be public both in terms of seeking commentary from law enforcement agencies and the public as to what needs to be done, what the issues are, and also in terms of the results being made public rather than just putting a bill before the parliament claiming that once again this is going to solve all the problems.

CHAIR—Ms Graham, part 3.2.3 of your submission refers to the extension of powers to a broader range of agencies, and I think you refer to lawyers and private investigators and so on. Would you like to comment on that aspect of the bill?

Ms Graham—Yes. That is obviously also a great concern for us because, once again, that is where this issue arises that we keep raising about a search warrant not necessarily being necessary. This is because, under the Telecommunications Act, section 280B et cetera allows ISPs and telephone companies to disclose information where it is required or authorised by law.

There is a situation in Australia at the moment where judges are granting orders to lawyers and private investigation agencies, particularly for the music industry, where the lawyers and

private investigation agencies are able to go into individuals' homes, ISPs' offices and telephone companies' offices and take copies, under the court order, of the entire hard drive of computers in those premises. The court orders are issued in secret. They are called Anton Pillar orders. Generally speaking, they do not appear to be made public even after the raid has been conducted. Certainly one cannot find them on SCALEplus's or AustLII's records of court decisions. One can find a couple but not very many. So, even though the court order clearly granted them the right to take what is called a bitstream image of the entire computer hard drive, one does not generally know whether or not that actually happened when they were on the premises because there is no information publicly available about what happened when this secret raid was conducted.

That is clearly a major concern for us. At the moment, when these raids are conducted at the University of New South Wales, Telstra's premises and so forth we trust that a copy of the entire email server of the ISP is not taken because to do so would include copies of undelivered emails; therefore, it would be an illegal interception. If this bill passes, there will no longer be any restriction legislatively on whether or not those court orders—that is, Anton Pillar orders—can authorise the taking of an entire copy of an ISP's email server. We find that very concerning because that would be occurring without a warrant. Granted, it would be a court order, but these court orders are very broad. When you are taking a copy of an ISP's email server this has nothing to do with the suspects; this is the email of every single customer of that ISP. We really feel that, until the laws about access to computer hard drives and so forth are vastly improved to ensure privacy is protected, we need the existing restrictions to stop things like Anton Pillar orders being able to be granted for the whole email server of an ISP.

CHAIR—The point that you make there links back to the point you were making in an earlier paragraph about accessing another person's undelivered messages ceasing to be an illegal interception and those people being completely vulnerable.

Ms Graham—Yes, that is right. At the moment, if a court is issuing an Anton Pillar order—

CHAIR—I am familiar with Anton Pillar orders.

Ms Graham—however it is used, the people who are executing it would be restricted by the Telecommunications (Interception) Act. But if the interception act ceases to cover undelivered emails then the restriction is removed.

CHAIR—Thank you very much for assisting the committee. Thank you also for your very broad-ranging submission. We understand, as you adverted to earlier, that we are operating in a very tight time frame and we appreciate the detail you have provided to the committee.

Ms Graham—Thank you very much. We were pleased to provide it and we would be pleased to provide anything else that may be of assistance as you continue your process.

CHAIR—Thank you.

[9.39 a.m.]

INMAN, Mr Keith, Director, Electronic Enforcement, Australian Securities and Investments Commission

PYNER, Ms Nicole, Manager, Enforcement Policy and Practice, Australian Securities and Investments Commission

CHAIR—I welcome representatives of the Australian Securities and Investments Commission. ASIC has lodged a submission with the committee, which we have numbered No. 4. Do you need to make any amendments or alterations to that submission?

Mr Inman—No.

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

Mr Inman—I have prepared a short introduction to provide additional context to our written submission. ASIC has over recent years made a number of submissions to various committees of review examining the issues surrounding lawful access to what has become known as 'stored communications' or 'stored message services'. ASIC's contribution to these reviews over those years has remained consistent.

ASIC has a broad range of regulatory responsibilities across the financial system, including a requirement to enforce the law as it applies to companies and the offering of financial services and products. When acting in its capacity as a law enforcement agency, ASIC investigates a wide range of contraventions against both Commonwealth and state statutes, including the Corporations Act and various crimes acts, for the purpose of obtaining criminal, civil or administrative outcomes.

In this regard, ASIC acts principally as a white-collar crime enforcement agency. We deal with fraud, misrepresentation, false and misleading statements and fiduciary negligence. Traditionally our investigations follow the paper trail, examining suspect offerings and suspect business transactions, often of a most complex nature. The evidence that we compile is predominantly oral testimony and source documentation. Our cases do not revolve around physical exhibits, such as knives, poisons, clubs or other objects capable of delivering physical harm. ASIC's enforcement cases revolve around objects that are capable of delivering financial harm, such as cheques, contracts, deeds, buy and sell orders, loan agreements, insurance policies and related correspondence.

Historically it has proven to be difficult to obtain the evidence of the sorts of white-collar crimes that ASIC investigates. For that reason, ASIC has been provided with wide-ranging investigative powers to ensure it has the means to effect its purpose. With the proliferation of stored messaging services such as email and voice mail, the paper trail can turn into a digital trail. Financial documents and business records that were once posted or couriered are now increasingly sent by electronic means. ASIC believes that the powers that have been vested in it should be sufficient to gain lawful access to these electronic documents and correspondence as they are in gaining access to paper based versions.

Our practical experience, however, indicates that they are not. The emergence of stored message services has created a dilemma for ASIC and the service providers. There is a lack of legal clarity as to when such documents and correspondence fall within the restrictions of the Telecommunications (Interception) Act and when they do not. With severe penalties attached to contraventions of the Telecommunications (Interception) Act, service providers have taken an understandably cautionary stance, and gradually over the past four or five years they have increasingly taken the view that telecommunication interception warrants are required before they will produce copies of stored messages to ASIC. Because ASIC is not an intercepting agency, this situation has led to a dilution of ASIC's investigative powers. It is now a reality that a fraudster could structure a business model around stored messaging services to the effect that ASIC no longer has access to the paper trail. For these reasons ASIC welcomes the clarification provided by the proposed amendments and supports the bill. Thank you.

CHAIR—Ms Pyner, do you have anything to add?

Ms Pyner—No.

Senator LUDWIG—Under what powers would you be able to access ISPs under this bill? Would you require a search warrant?

Mr Inman—In certain circumstances we apply for search warrants. We apply for search warrants under the Commonwealth Crimes Act or under our own legislation. We also have compulsory notices, which, in the physical world, would be sufficient to gain access to business records. There are also provisions of the telecommunications act, depending on the nature of the information that we are seeking from ISPs.

Senator LUDWIG—And consent, of course.

Mr Inman—And voluntary consent.

Senator LUDWIG—As I understand it, that would mean that you would then be able to access both the accessed and unaccessed emails of an intended target from an ISP. Would that be right?

Mr Inman—We would prefer to have access to emails, whether they have been accessed or not. We believe it is analogous to the situations where we can obtain business records that are in an envelope, whether they have been opened or not.

Senator LUDWIG—You mention in your submission—at least, you seem to argue—that, because of the opacity of the law at present, it is unclear to you what the law currently is and, as a consequence, there may be instances where the culprits are getting away with it. Can you give the committee an idea of what you mean by those powers, how they will be used and how they might be impeding your current investigations?

Mr Inman—I can think of a number of examples that would be useful in answering this question. The first is that in a recent investigation we became aware of an Australian business that was actually a global business, where 90 per cent of the infrastructure supporting that business was in fact based overseas. The means by which the directors and officers of the company coordinated their business activities was principally through the use of emails. That indicates that, as we transition to the electronic commerce environment, these new business models will take more and more advantage of the cost savings, the efficiency gains and,

obviously, the cost benefits from structuring their business in the global sense and will make more and more use of emails.

I am also aware of examples where, on major high-profile matters, proof of the intent of directors to commit offences has been provided by obtaining copies of emails that show deliberations and offline discussions between directors indicating that they knew about certain circumstances. Those emails will become a key element of our criminal prosecutions when those charges are finally brought before the courts. Finally, to give another partial insight into the question that you raised, I can think of another example where an insider trading allegation involving a broker came to an end because the ISP that we approached using compulsory notices declined to provide access to emails because it was unclear whether the emails had been opened by the owner. In essence, that insider trading investigation finished there.

Senator LUDWIG—In relation to compulsory notices, do you believe you currently have the power to access opened emails with an ISP?

Mr Inman—We believe we do. Unfortunately for us, there are not many ISPs that share our view.

Senator LUDWIG—Have you spoken to the Attorney-General about this issue?

Mr Inman—We have had consultation over quite some time with the Attorney-General's Department, informing it of the situation. I know that the Attorney-General's Department has sought to clarify it with a number of ISPs. However, ISPs still err on the side of caution. ISPs, particularly the large ones that I have been dealing with, believe that—and this is a general statement—the situation is unclear and, until such time as clarity is provided, they are going to err on the side of caution and will ask for interception warrants.

Senator LUDWIG—And the Attorney-General's Department's view is that you do have the power under a compulsory notice? Have they indicated to you what their view is?

Mr Inman—I know the Attorney-General's Department will be giving evidence.

Senator LUDWIG—Yes, I will be able to ask them as well, but they must have communicated to you their view about this issue. They would have said either, 'Yes, you do have the power,' or 'No, you don't.'

Mr Inman—The Attorney-General's advice to us is that we do not have the power where the emails are unopened.

Senator LUDWIG—But what about in respect of where the email has been opened and can be identified on the ISP server?

Mr Inman—Then we have the power to use our compulsory notices. Our problem then is that ISPs do not believe that they can say with any degree of certainty whether an email has been opened or not, and they therefore decline to respond.

Senator LUDWIG—Have you sought clarification in the courts in respect of that issue?

Mr Inman—No, we have not.

Senator LUDWIG—Why haven't you? How long has this been going on for?

Mr Inman—Increasingly since about 2000.

Senator LUDWIG—So it has been an issue for the last 3½ years?

Mr Inman—That is correct.

Senator LUDWIG—Have you sought clarification with the Director of Public Prosecutions about the issue?

Mr Inman—We have worked with various agencies through fora like the AGEC—the Action Group on Electronic Commerce. I think it is fair to say that there are various views in existence and various legal advisings as to the possible interpretation of the Telecommunications (Interception) Act. In fact, they probably add to the confusion rather than clarify it.

CHAIR—I was going to say I was not sure what that meant, Mr Inman, so I am glad you said it!

Senator LUDWIG—I thought I would leave it alone! This bill would enable ASIC to access stored communication on an ISP server which apparently has been opened, but you indicated earlier that the ISP cannot identify whether it is opened or unopened.

Mr Inman—I have spoken to three ISPs and the Internet Industry Association, who tell me that they cannot always tell if an email has been opened or not.

Senator LUDWIG—So this bill will operate to do what, in your view? It will allow you to access all communication whether opened or unopened on an ISP?

Ms Pyner—I believe that is correct, yes.

Senator LUDWIG—That would be for all compulsory notices irrespective of the seriousness of the crime involved?

Ms Pyner—Yes. At least some of our compulsory notice powers are quite restricted in terms of what we could require production of, but they do not actually require that an offence has been committed or that we have suspicion that an offence has been committed before we can serve them. To clarify my previous response, I think that that is correct except in cases where the email is still in transit and is basically bouncing from computer to computer before it reaches its final home. In those cases this bill would not allow us to access those, because that is subject to an exception under the provision.

Senator LUDWIG—I am not sure I know what that means.

Ms Pyner—My technical knowledge is somewhat limited, but my understanding is that, as a technical matter, when an email is sent it goes from one computer to the computer that is its final delivery point, but in the meantime it can bounce from computer to computer across the Internet. My understanding is that that is how the Internet basically works. So it can make a few stops before it arrives, but those are momentary—very short. It is not anticipated that this bill would allow interception without a TI warrant along that trail when it is just making the momentary bouncings, but once it has been stored—once it is sitting on a computer for a period of time and is stored, either before or after it has been read—we would be allowed to access the emails.

Senator LUDWIG—So that is both at the individual computers and the ISP, and the sender?

Ms Pyner—The sender, the recipient and the ISP, and indeed any other computer that for whatever reason it happens to be stored on. But it has to be stored; it cannot be in transit.

Senator LUDWIG—When would you know to draw the line and say, 'This requires a telecommunications interception notice'?

Ms Pyner—The question of us intercepting emails in transit just simply would not arise—we would know that we would not be able to do that and so would the ISPs. We cannot get telecommunications interception warrants and we do not have access to material that has been intercepted by other agencies.

Senator LUDWIG—You cannot envisage a circumstance other than an email in transit where you would not be able to access it and therefore would not require a telecommunications interception warrant?

Ms Pyner—I believe that is correct, yes.

Senator LUDWIG—What about SMSs or telephones? Would the same apply?

Ms Pyner—The same, effectively, applies. If it is actually on the network in transmission from one phone to another—and I confess I have less understanding of the technology of how this works—we would not be able to intercept it. But once it is stored on some sort of equipment, be it either the phone or some sort of equipment in the carriage service provider's premises, then we would be able to access it.

Senator LUDWIG—Would that be through a compulsory notice to produce the phone?

Ms Pyner—It could be any of the four mechanisms that we discussed earlier: a compulsory notice under our legislation, a search warrant, a notice under the Telecommunications Act or consent.

Senator LUDWIG—That is for any compulsory notice for any offence that you believe has been committed?

Mr Inman—The focus for us is always—

Senator LUDWIG—Do you see? It is very broad.

Mr Inman—We have broad powers. Our powers are to gain access to business books and records, and they are very broadly defined. We have many cases that provide clarity on just how broad the definitions of 'books' and 'records' are for businesses. In the physical world that is the reality. We have needed to rely on those powers in order to compile the evidence needed to substantiate all of the offences that ASIC administers. Our offences range from fines through to 10 years under the Corporations Act and, of course, under the more serious offences in the Crimes Act, there are very large sentences of imprisonment.

To respond to the suggestion of how broad our powers are, our powers are necessarily broad. They relate to the books and records of companies and to transactions in the financial system. We have lots of case law as to how broad the terms 'books' and 'records' are to be interpreted and we believe that they should provide us with access to those same books and records, even if they are held in an electronic state as a stored message.

Senator LUDWIG—Thank you.

CHAIR—Thank you very much. Before we wind up, Mr Inman, if ASIC were to get the powers that are proposed in this bill, what guidelines do you have in place to deal with the privacy of third parties?

Mr Inman—There are multiple guidelines and checks and balances that are in place for all of our access powers. Our notices can be challenged and are regularly challenged in court as to the propriety of their content. We are regularly asked to substantiate our notices and we do that with very high success rates. We also have record-keeping guidelines that ensure continuity of evidence. From the moment that evidence or potential evidence comes into our hands it is logged and stored.

Our access powers to information are also reviewable by the Privacy Commissioner. ASIC has been subject to a number of privacy audits around the country by the Privacy Commissioner's staff over the years, specifically reviewing and auditing the propriety of our information collection and our evidence collection. We are also reviewable. Many of our decisions are reviewable—our administrative decisions under the AAT—and those reviews can also look at the propriety of our access to documentation. There are many layers of review and supervision of ASIC's access powers, including not least the ability to challenge our notices in the court.

CHAIR—What guidelines does ASIC have in place within the organisation to limit the range of officers and staff who have the opportunity to view the sort of material we are talking about—particularly material that pertains to third parties who may not be directly connected with the ASIC investigation?

Mr Inman—Our evidence handling system, which is partially computerised and partially file based, has security built into it. The investigation teams are only provided with access to their repository of evidence. In matters that are considered to be highly protected, the degree of access is limited to individuals within the teams. Because we recognise that when we obtain evidence we are in essence holding the property of third parties and we have obligations for that, our security and administrative guidelines require us to secure that information. We follow the protective security manual in the classification and handling of documentation. As I mentioned earlier, we also have continuity requirements, which require us to ensure and restrict access and the security of documents and to record who has access to those documents and when. Our computer systems log access to electronic evidence, including images of documentation that we might obtain as evidence.

CHAIR—Are any of the guidelines to which you have referred set down in a manner that you can provide to the committee?

Mr Inman—Yes. We are happy to make that available.

Ms Pyner—The manual I expect Keith has in mind is confidential. We are happy to provide it to the committee, but we would not want it to be made public.

CHAIR—We would gratefully receive any material that can be made public, and we will consider that and come back to you.

Ms Pyner—The reason is that the manual we have in mind sets out the manner in which we protect this sort of information. We would not like that to be published, because that might threaten the protection of that sort of information.

CHAIR—It does not make it easy for us. Thank you very much for your assistance to the committee this morning.

[10.04 a.m.]

ARMSTRONG, Mr Paul, Acting Deputy Privacy Commissioner, Office of the Federal Privacy Commissioner

PILGRIM, Mr Timothy Hugh, Acting Federal Privacy Commissioner, Office of the Federal Privacy Commissioner

CHAIR—The Office of the Federal Privacy Commissioner has lodged a submission with the committee which we have numbered No.6. Do you need to make any amendments or alterations to that submission?

Mr Pilgrim—No, we do not.

CHAIR—I ask you to make an opening statement and we will go to questions at the conclusion of that.

Mr Pilgrim—Thank you for the opportunity to appear before the committee. I only have a brief statement, and it puts into context our office's view of this issue. Without wanting to sound trite, the issue generally is very complex. It is complex for our office to get across and I am sure it is complex for all those agencies performing important law enforcement functions for the broader community. But it is also an issue which impacts dramatically on the community because it goes to the heart of accessing personal communications. Many of those personal communications in the past have been done by voice—by phone. Through new technologies we are now seeing a move for the community to start using new means of communicating personal messages—via email and via SMS. There is a question at large, which is: does the community as a whole understand how well that information is protected or in fact if there are going to be any changes to that protection?

The challenge facing the community is the same as the challenge facing the committee at the moment—that is, what level of protection should be given to that information? Should it change simply because the means via which it is being transmitted and stored are changing or should it maintain the same level of protection as is afforded to voice communications? For that reason, we certainly welcome the comments made by the Attorney-General that there should be a review in 12 months into this particular issue. However, we start from the premise that communication, whether stored or via voice, should be afforded the protections offered by a telecommunications interception warrant as the starting point. Once there has been a comprehensive review and hopefully a review that includes broad public consultation, we may then all be in a better position to make a judgment of whether those protections should change.

CHAIR—Mr Armstrong, do you have anything to add?

Mr Armstrong—No.

Senator LUDWIG—You have had the opportunity to listen to ASIC. Does the way they will handle the new power granted provide you with enough safeguards or do you remain concerned?

Mr Pilgrim—I suppose the issue for us is one of seeing how a new law is applied once it is in place. We certainly understand that ASIC has considerable guidelines in place, as was mentioned by the representatives of ASIC. We have done audits of their organisation in the past and on the whole through those audits we have been quite satisfied with the various protections for the personal information they collect. On that basis, we would not assume that they would be dramatically changing the protection of the personal information they collect.

The question goes back to what level of protection this sort of information should have, being stored communications in the first place. We would prefer to see the protections offered by telecommunications interception warrants as providing a higher level of protection in the first place for organisations such as ASIC and other law enforcement agencies to get access to that information.

Senator LUDWIG—In relation to the review that is being mooted by the Attorney-General, do you have a view about its terms of reference, how broad it should be, and whether the law should remain as it is now—whatever that night be—or move to the new regime proposed by this bill and then be subject to a review?

Mr Pilgrim—Our view is that the law should remain as it is if—

Senator LUDWIG—If it can be clarified—

Mr Pilgrim—we all agree that stored communications would require a telecommunications interception warrant to get access to that information. I believe it is not a position generally held by the community that they would be aware of the level of protection that is afforded that sort of information at this point in time. I am sure that quite a large percentage of the community is aware interception warrants as such would be needed to access their telephone calls. Leading on from that, those people could assume that the same level of warrant is required to access any information that is transferred across telecommunications systems, regardless of whether it is SMS or email. For that reason, I would suggest that our office believes that the level of protection should stay as under the telecommunications interception warrant regime until such time as there has been a fulsome review—as I commented in my opening address, a comprehensive review and one that can have to the greatest degree possible involvement from the broader community.

Senator LUDWIG—In respect of the privacy concerns, can you outline some of the issues that you may have already encountered in relation to emails and third party privacy issues? Have any come across your desk that you can talk about, more in the broad rather than the specific?

Mr Pilgrim—If we are talking quantity, I could not say that we have had a huge number coming through the office at all in regard to interception of emails and the like, for a number of reasons. Firstly, if an issue is coming up that is directly related to, say, telecommunications interception—whether it be through the interception act or access to a person's phone records under the Telecommunications Act—a lot of that information would possibly go to the Australian Communications Authority in the first instance. Secondly, in the case of a challenge against warrants and the like, that is an issue that the Ombudsman's office would be dealing with through, say, a complaint from an individual. We do see some issues relating to complaints of a breach of privacy in regard to email. Those have been limited to the

disclosure of emails, say, from one organisation to another when there was an assumed inappropriate message or information being released, and, under our regulating responsibilities with the Commonwealth government agencies, we have seen that come up on a number of occasions where one agency has released an email to another agency that has been sent by the former agency's employee.

Senator LUDWIG—In respect of those privacy rights themselves, which ones do you say would be breached or potentially breached under this legislation if it were to pass?

Mr Pilgrim—When you say breached under this legislation—

Senator LUDWIG—You have got a number of national privacy principles. If the legislation passes, then TI warrants, at least, are not required for stored communication. So TI warrants are only then required for live telecommunications or perhaps transitory ones such as chat rooms, although I might still need to clarify that with the Attorney-General's Department. Therefore you have access by ISPs of stored communication, you have access by other agencies outside of the AFP and you have access to third party as well by those agencies, including ASIC. Where do the national privacy principles then interact at that point?

Mr Pilgrim—The starting point for the interaction, if we take it from a scenario where, say, a law enforcement or revenue agency—any of that group; let's use ASIC as an example—makes an approach to an organisation to get some records about an individual that may be being transferred through an ISP, the ISP would need to consider its responsibilities in that scenario under the national privacy principles and, in particular, national privacy principle 2. National privacy principle 2 deals with the use or disclosure of personal information. The ISP would need to be comfortable that the agency requesting that information had legitimate power to do so, be it through some authorising power within its own legislation or, in fact, through a warrant issued either under the TIA or under the TA to access that information. The ISP would need to be satisfied that the requirements of national privacy principle 2 were met that the disclosure in that case would be authorised or required by law. Having satisfied themselves that either there was the power within the agency's own act or there was an appropriate warrant, they could disclose the information in those circumstances.

Senator LUDWIG—Under this bill, then, ASIC, lawfully seeking a compulsory notice to produce details of all read emails from an intended target, would be able to lawfully access all of those. It would be in accordance with principle 2 in that it is a lawful pursuit because it is potentially investigating an offence.

Mr Pilgrim—That is correct. If the authorisation power was within ASIC's act then that would enable them to access information.

Senator LUDWIG—And that would include all third-party or any other communication that might not be relevant to the offence?

Mr Pilgrim—The issue then comes down to a question of relevance, as you are suggesting. They would need to be very careful about the third-party information they were collecting to make sure that it was particularly relevant to the case they were investigating; otherwise, they would need to question whether they could in fact take information from the ISP about the third party. If it was difficult to then separate off, they would need to ensure that that received the appropriate level of protection once it was stored and kept by ASIC.

Senator LUDWIG—Has the privacy commission done an audit of ASIC to see whether or not their systems and programs at least comply with privacy commission principles?

Mr Pilgrim—We have in the past done audits of ASIC. I cannot remember the exact date of the last one. I suggest it was a few years ago. As you are aware, we have not undertaken many audits at all in the last two to three years of government agencies, for reasons of having to reallocate resources within the office.

Senator LUDWIG—Yes. They can always ask on a fee-for-service basis though, can't they?

Mr Pilgrim—That is an interesting question, and one we have not pursued entirely. Off the top of my head I would assume that they could perhaps ask us to go and do an audit of them and offer to pay us to do it. We have entered into similar agreements with the Customs office, as you may recall from estimates hearings. So I would assume that, yes, ASIC could be in the position, if they were willing to fund us on a resource level, to get us to go in and do audits.

Senator LUDWIG—And what about the AFP; have you done an audit of them recently?

Mr Pilgrim—Again, not recently, but we have done audits of the AFP in the past.

Senator LUDWIG—All right. Thank you.

CHAIR—Was the Office of the Federal Privacy Commissioner consulted in the development of this piece of legislation?

Mr Pilgrim—I will just check with the acting deputy commissioner. I believe that we did have drafts of the legislation at various stages.

Mr Armstrong—I believe we were given a draft of the legislation about two days before its tabling in the House.

CHAIR—That is more an information than a consultation.

Mr Armstrong—We did not have a lot of time to analyse the provisions, no.

CHAIR—Did you provide your views to the department?

Mr Armstrong—I believe we did.

CHAIR—The risks that you identify in your written submission are twofold in terms of the effect of the bill on private communications. The one that I would like you to comment further on is what you refer to as:

... a shift in the balance between the private nature of personal communications and the ease with which law enforcement bodies and some government agencies can intercept such communications.

How do you see that playing out in the fullness of time?

Mr Pilgrim—Again that goes to the heart of one of the comments I was making in the opening statement, which is how we are seeing the community's use of telecommunications systems moving on and the community adopting new technologies such as email and SMS and whether or not there is an assumption within the community that those types of telecommunications systems and the way people transfer information are going to receive the same level of protection as does transmission of voice messages. I am not sure, and I do not think our office has any firm evidence one way or the other, whether the community does

have an understanding of what level of protection there is of that information. As I said, we do believe, though, that the community has very strong views around the protection of voice communications and can infer that there may be a view that there is an expectation that SMS messages and emails would receive the same level of protection.

One of the risks is that, if people do have an assumption that emails and SMS should be protected in the same way and are not going to receive that level of protection, we could in the future, I would assume, see a dramatic drop-off in the use of email and SMS as a means of communicating general conversations. Again, that is an assumption, and I acknowledge that. But it is a potential risk. When the privacy legislation was being developed some years ago, there was concern in the community about online shopping and other e-commerce activities because people did not trust the communication systems to provide a level of protection for their personal information. Hence, Australia and a number of other countries moved to introduce tougher laws around the protection of the privacy of the information that was being transferred. We could assume that there could be a backlash from people who are not willing to use SMS and emails to transfer day-to-day communications, because they will become nervous about what level of protection is afforded to those particular transmissions of information.

CHAIR—From the perspective of the Office of the Federal Privacy Commissioner, should people have an expectation that they will be able to communicate in private on the assumption that they are doing nothing wrong?

Mr Pilgrim—We certainly feel that people should be able to assume that they can have a conversation in private—be it voice, email or SMS—without fear that it is going to be intercepted.

CHAIR—I do not think you have made any specific observations on the potential impact of the bill, if enacted, on uninvolved third parties. Do have any comments to make on that?

Mr Pilgrim—The only comment I would make is that, yes, that is a risk and we do not pick it up in this submission. We have dealt with it in the past under other aspects of telecommunications laws. We believe there is always a risk in regard to the transfer of any communication that the information of third parties—who may not be aware that their information is being collected—will be collected and they will have no understanding of where it is going and how it is used.

CHAIR—If you wanted to make any further comment on that, I would be happy for you to take that on notice, examine it further and come back to the committee.

Mr Pilgrim—We will do that.

CHAIR—Thank you for appearing today.

[10.23 a.m.]

BATCH, Federal Agent David Alan, Senior Legislation Officer, Australian Federal Police

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

OLSON, Federal Agent Brian John, Manager Information Technology, Australian Federal Police

VAN DAM, Mr Trevor Anthony, Chief Operating Officer, Australian Federal Police

WELDON, Federal Agent Kylie, Senior Legislation Officer, Australian Federal Police

CHAIR—Welcome. The AFP has lodged a submission with the committee, which we have numbered 7. Do you need to make any amendments or alterations to that submission?

Mr Van Dam—No.

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

Mr Van Dam—The AFP appreciates the opportunity to appear before the committee in relation to the inquiry into the provisions of the Telecommunications (Interception) Amendment (Stored Communication) Bill 2004. The commissioner has asked me to extend his apologies to the committee for not being able to attend today. He is presently out of Canberra on business. Accordingly, I will be making this submission on behalf of the commissioner. In summary, and as previously put by the AFP to this committee, it is becoming increasingly common for serious offenders to use computers to store and communicate information in the course of conducting their illegal activities.

It is important to the detection and prosecution of offences that AFP officers are able to search the content of computers and to gain access to stored communications expeditiously. The AFP raised these and other imperatives during the committee's previous inquiries into proposed telecommunication amendments. The amendments proposed in the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 will clarify that a telecommunications interception warrant is not required to access stored communications such as voice and email. Under the proposed provisions, it will no longer be an interception for the purposes of the Telecommunications (Interception) Act for a person to access communication at a point where it is stored. As a result, access to a document or other stored communication will not require a TI warrant just because it happened to be sent by email or stored on a remote server. This has the practical effect of ensuring that law enforcement may access stored communications where the officer holds an appropriate search warrant or other form of lawful authority.

The AFP welcomes this clarification and the practical solution that it provides for the effectiveness of investigations into serious Commonwealth offences, such as terrorism and people-smuggling. From the AFP's operational perspective, the amendments will ensure that investigators are not required to obtain two warrants to conduct a single search. AFP concerns about the two-warrant scenario centred on the potential that important evidence could be put

at risk. Without the amendment allowing expeditious access to stored communications, highly disposable and easily destroyed forms of evidence could have been lost during the time taken to access the requirements to obtain TI warrants. Obtaining TI warrants as a matter of course prior to every search would have resulted in an unnecessary and onerous burden on limited Commonwealth resources.

The committee will recall that the AFP was also very concerned that appropriate corporate governance activities should be able to be undertaken without the requirement of a telephone intercept warrant in each case. These activities include monitoring employee emails in compliance with acceptable use policies and scanning in real time to protect AFP information systems against viruses and other malicious code. By allowing access at the point of storage or through permission, the proposed amendments will ensure that the AFP can run its professional standards and employee integrity regimes without breaching the provisions of the telephone intercept legislation.

As the committee is aware, the Attorney-General's Department will be undertaking a comprehensive review of the entire telephone interception regime over the next 12 months. The AFP welcome that review, and we will monitor the application of the amended provisions leading up to the conclusion of that review. We see that as a vehicle to raise any matters that might emerge in the practical application of these. In closing, the AFP would like to reiterate the operational requirements that underpin the need for stored communications amendments and our support for them.

CHAIR—I think at the conclusion of your remarks then you said that the review would be an opportunity for people to raise concerns. Perhaps you could go back to what you said just then at the end of your statement.

Mr Van Dam—What I was saying was that, as the committee is aware, the Attorney-General's Department will be undertaking a comprehensive review of the entire telephone interception regime over the next 12 months, and we welcome that. The AFP will monitor the application of the amended provisions over the course of that period and any concerns that arise in the context of practical application of that will be fed into that review.

CHAIR—Unless you have been a victim in the previous 12 months. It is a bit late for you then.

Mr Van Dam—I think, if these matters emerge during the course of that review, we will be looking to put them in as they arise.

CHAIR—Because, for third parties whose communications may be accessed or about whom information might be revealed completely unbeknownst to them in the 12-month period, they will not have any protections or have their concerns addressed in the manner to which you adverted, will they?

Mr Van Dam—If we go to our understanding of the effect of these provisions, access to stored communications will still be undertaken in the context of lawful authority.

CHAIR—With a search warrant?

Mr Van Dam—With a search warrant.

CHAIR—But not with a telecommunications interception warrant, which requires some consideration to privacy issues to be given.

Mr Van Dam—I think that is premised on an assumption that there are no privacy considerations within the search warrant framework. Notwithstanding we can access material, there are still protections within that framework for individuals as to the use of the material that may be there for—

CHAIR—But they are not as formal as they are under the TI Act—that is my understanding. The TI Act itself requires some reference to or consideration of privacy issues before an interception warrant is obtained in a number of instances.

Mr Van Dam—I might pass to Kylie on that.

Federal Agent Weldon—Under a search warrant, the owner of the information is afforded certain rights and so would be aware of our access to those communications.

CHAIR—Sorry—how will a third party whose information is being accessed under a search warrant that is provided for under this bill know that their information is being accessed and be able to exercise their rights?

Federal Agent Weldon—So, the intended recipient if we are executing—

CHAIR—No, the owner of a third party communication—

Federal Agent Weldon—The person who communicated it?

CHAIR—who has no involvement at all—whatsoever—in your investigation.

Federal Agent Weldon—When we execute the search warrants, it is the communication that is made to the intended recipient or from the intended recipient that would be made available to us. The person who is the subject of the search warrant would be able to be present during the search and would be given a receipt which records all the evidence that was obtained while executing the search warrant. That person might be able to communicate that information to the communicator of the email communication. We do create records, when we seize the evidence, that may be admitted in court and are also subject to the information privacy principles under the Privacy Act. So we are restricted in terms of what we can do under the Privacy Act. Also, any unlawful disclosure or any unlawful use of that information may be subject to criminal and disciplinary action under the Crimes Act or the Australian Federal Police Act. So, those protections are afforded. We also have exhibit handling guidelines to protect the use of that information.

CHAIR—So that I can clarify, did you just say that the person who is the subject of the search warrant might be able to help out by telling the people who have been communicating with them that their communications have been the subject of a search warrant? Is that what you just said?

Federal Agent Weldon—That may happen. It depends on the communication we are dealing with, but the person who was the occupier of the premises would be made aware at least, or the person whose equipment we were accessing would be ordinarily made aware.

Senator LUDWIG—'Ordinarily made aware'—when would they not be made aware? You do not always make people aware that you are accessing a computer under a search warrant,

you are on the premises and you are taking a print of the computer, do you? You are not required by law to tell them you are there if you have a search warrant.

Mr Van Dam—For a search warrant at premises, our normal practice is to afford the person to whom that warrant is being served the opportunity to be present. Likewise, our normal practice is to generally take computer equipment away without interfering with it on the premises, and in those circumstances the person affected is in fact given a receipt for goods removed.

Senator LUDWIG—You used the word 'ordinarily'; you are not required to by law, though.

Mr Van Dam—Our own guidelines and provisions have it as an expectation that that will be the norm.

Federal Agent Weldon—The legislation provides that if the occupier is present a copy of the rights of the occupier must be provided to them. Our practice is that if the occupier is not present we get an independent person or take all measures to try to locate the occupier. Where we cannot locate the occupier we either execute it at another time or we get an independent person like a JP to accompany us.

Senator LUDWIG—Does that happen in all instances?

Mr Van Dam—I could not give you an absolute statement that it happens in every single instance, but it would certainly happen in the majority of instances. It is the general practice.

Federal Agent Lammers—In the majority of cases the occupier or the lawful owner of the premises is there and that person is served a copy of the search warrant. In the extraordinary circumstance that that person might not be there, another person is used to oversight the execution of the warrant.

Senator LUDWIG—So there are instances where you access a computer for, in this instance, likely emails where there is no occupier there, and you have the ability to access emails under this proposal with a search warrant and the only person that may be there is a justice of the peace that you have brought along?

Federal Agent Lammers—That is possible, yes.

Senator LUDWIG—What of the issue of the protection of third parties—for those people whose emails are accessed who are not part of your investigation? They are not notified at all, are they? Does the JP view the emails as well to see what is on them or does he just oversee the process?

Mr Van Dam—As I indicated, it is not our normal practice to interrogate the computers on the premises. In fact, it is generally not good forensic practice to do that.

Senator LUDWIG—What do you do—take a copy?

Mr Van Dam—We usually take the computers away and, where appropriate, take a copy of the hard drive.

Senator LUDWIG—What happens in relation to the privacy of a third party who is not subject to investigation? You will then have records which include the copy of the hard drive

with emails and the like from a whole range of people other than those who are being investigated.

Mr Van Dam—To the extent that any material gathered in the course of that search warrant does not relate to the specific investigation being conducted, that material is not retained. Under normal search warrant provisions, the obligation is in fact to return that material. We use a parallel to, for example, correspondence. If the correspondence is not related to the activities being investigated, that correspondence is returned and the AFP has no particular interest in it. That would be the same in these circumstances. To the extent that that correspondence may then be relied on in the course of a prosecution—and if I use the analogy of a letter—there is no obligation, as I understand it, to inform the sender that that material is now in police possession, unless we were going to rely on that material, in which case we may well go to the sender. In fact we may in some circumstances find the sender being brought into our investigations as a potential suspect.

Senator LUDWIG—The last time we were here in relation to this particular issue there was disagreement between the Attorney-General's Department and yourselves in relation to the application of 3L under the Crimes Act. Has that been resolved?

Mr Van Dam—The advice I have received is that these amendments will clarify that sufficiently for the purposes of our operations.

Senator LUDWIG—But if this bill is not passed, how will the difference be resolved? Has it been resolved at the moment or does it still remain unresolved—the application of 3L in your view and the view of the Attorney-General?

Federal Agent Weldon—It will remain ambiguous.

Senator LUDWIG—Could you explain to me what your view is now?

Federal Agent Lammers—Our view has always been that, under the search warrant regime, 3L allows us lawful access to materials at premises upon which we execute search warrants. The AFP's position on that has not changed.

Senator LUDWIG—Does that includes emails, both read and unread, on a computer?

Federal Agent Lammers—Yes.

Senator LUDWIG—Does it include SMS messages on a telephone?

Federal Agent Lammers—Yes, that was our understanding.

Senator LUDWIG—Have you had discussions with the Attorney-General since February about the differing views in respect of that provision?

Mr Van Dam—We clearly had discussions in the context of these amendments. As I understand it, there are differing opinions on this question.

Senator LUDWIG—There seem to be.

Mr Van Dam—There are two dimensions to this. One is that we are not aware that the matter has been tested in the courts. So there are differing opinions, but to date they have not been tested. From our perspective, and I think from the department's perspective, the intention here is to try and bring these matters beyond doubt.

Senator LUDWIG—It is just that I could not see in the explanatory memorandum or the Attorney-General's second reading speech how those competing views in relation to 3L and the application of this legislation were resolved. Do you say now that this bill is designed to resolve the difference between your view and the DPP's view of how 3L should or should not apply?

Mr Van Dam—These amendments will remove that core area of ambiguity.

Senator LUDWIG—You say 'core area'. Is there still ambiguity outside of the core area?

Mr Van Dam—No. Perhaps it was a poor choice of words. To the extent that the ambiguity about the application of 3L exists, I understand these amendments will resolve that.

Senator LUDWIG—So, should this legislation pass, the only time that you will be required to get a telecommunications interception warrant will be in relation to voice over Internet protocol and telecommunications telephones and mobile phones.

Federal Agent Lammers—That is correct—in its transit over the telecommunications system.

Senator LUDWIG—You can then access stored opened and unopened emails. Is that your understanding?

Mr Van Dam—As long as it is stored and not transitory in the terms of the amendment.

Senator LUDWIG—What do you call transitory?

Mr Van Dam—I am relying on the definition in the amendment.

Senator LUDWIG—What is your understanding of that bit?

Mr Van Dam—You are getting me into some highly technical, complex areas.

Senator LUDWIG—It is the law you are going to apply.

Mr Van Dam—I understand.

Federal Agent Lammers—Where it is momentarily stored and buffered for that very small portion of time, our understanding is that that particular scenario is caught by the provisions of the TI act. Where it is actually stored and then accessible as being stored, the amendments allow lawful access to that stored communications. The difference is that, where it is almost instantaneously passing over the telecommunications system, it would be caught by a TI warrant; where it is not and is stored, we suggest that these amendments allow us to have lawful access to that information.

Senator LUDWIG—So the case of, for example, a chat room, where two people are typing to one another about matters you might have an interest in, what is required in that instance—a telecommunications interception warrant, a warrant to the ISP or consent?

Federal Agent Lammers—Given the nature of a chat room, where the conversation is backwards and forwards and fairly imminent, the application of the TI act would apply. That is, we would need a warrant to intercept chat room activity. When the content of the chat room is stored on the server and becomes stored information, then it should be accessible by a search warrant.

Senator LUDWIG—How long is the time interval? If you are using a chat room, as I understand it—although I cannot say I have used one recently—you type something in; someone responds; then it continues to build. So someone can then go back five minutes later and see what the conversation was between various people in that chat room. At what point does it become stored so you can access it—30 seconds, a minute or five minutes after they have used the chat room? Or do you say that all chat room stored is inaccessible? It seems that you are saying some of it is. I was just curious as to at what point you say a telecommunications interception warrant is required and at what point you cease to require one?

Federal Agent Lammers—That part of the chat session that is finished in almost real time becomes stored if in fact that is how the ISP deals with the information. Given that not all ISPs store all information permanently—it all depends on their storage capacity—the immediate chat sessions between people happening in almost real time are caught by the TI act. Where it is stored, the chat has finished and it is still resident on a server, it is caught by the search warrant regime.

Senator LUDWIG—The other area that was of concern was the AFP monitoring of internal emails. The previous bill, in your view, as I recall, seemed to rule out the ability for the AFP to examine internal emails without a TI warrant. The Privacy Commission noted in their submission in relation to the current bill:

> The Office agrees that it is appropriate for owners and operators to be able to protect their computer networks against malicious software, such as viruses, and to undertake content monitoring under certain conditions.
>
> If there is continued legal uncertainty about whether such activity may contravene the Interception Act, this could be resolved by amending the legislation to ensure that while protection is maintained for personal telecommunications generally, e-security and corporate governance measures are permitted.

So in short you could have an exception that where you are doing AFP, ASIO or ASIC, for example—perhaps not—you might be able to then have an exception so that they would not require a telecommunications interception warrant or corporate governance or e-security measures in relation to internal emails. Would that not be a better way of proceeding?

Federal Agent Olson—In relation to the integrity of the network and the good order and management of the network, there are sometimes some automated processes that take place where you do not actually have a human viewing the material. In other cases it may be necessary to, say, retrospectively look at some traffic to identify problems that might be causing performance issues and, as you said, to identify malicious code and so on. There is no specific exclusion in the amendments so as far as the AFP is concerned. This all happens once it is in the AFP's domain. The owner of that system is the Commissioner of the Australian Federal Police, therefore we have a responsibility to do what is necessary to look after the integrity of the network, and that may or may not require some human intervention.

Senator LUDWIG—I understand that. To resolve that, you could have an exception to the telecommunications interception regime where the AFP or ASIO could access, as a way of dealing with that issue rather than providing carte blanche access to all emails whether unopened or opened on an ISP or internal server. It is just an alternative way of dealing with it. That would satisfy your concern. In terms of the AFP monitoring their emails for the range

of issues that you have mentioned, including e-security and corporate governance, you could deal with it by an exception under the TI warrant to allow the AFP to deal with it that way and that would resolve your concern in that area, wouldn't it?

Federal Agent Olson—Yes, or we could also deal with it by consent; that is, having employees—

Senator LUDWIG—Sometimes you do not want consent though because you might be conducting an investigation. That was explained to us the last time we were here. I acknowledge that. Would you be able to remotely access computers and their emails under a search warrant regime under this bill? I am just trying to understand the range of powers this bill might provide you with.

Mr Van Dam—Forgive me, Senator, but when you say 'remotely access', are you suggesting that we can sit in an office and somehow remotely enter someone else's computer and then start downloading material?

Senator LUDWIG—Yes. I can access my computer remotely. I do not have to be in front of it to access it. Software is available. My computer obviously knows that but I may not.

Mr Van Dam—To the extent that the search warrant is effected on a place, I do not think these provisions would—

Senator LUDWIG—There is the ability to have software to do that and there is also keystroke monitoring and a whole range of other spyware. I am not up with all the computer jargon that goes with it but I suspect some of your technical officers might be. So there is the ability to access keystroke monitoring. There is the ability to access computers remotely in either a limited or a wider capacity. Will this bill allow you to do that?

Mr Van Dam—To the extent that that sort of keystroke monitoring that you are describing did exist at all it would very much be real time and, as such, would be picked up under the telephone intercept type provisions.

Senator LUDWIG—Keystroke monitoring records all your keystrokes in a given period and you can remotely access that, download it, and then examine that and in doing so you can then reconstitute—this might be a poor way of explaining it—what has transpired on that computer.

Federal Agent Lammers—The answer to your question is really not difficult but it is an answer that we would probably prefer to give in camera because, in answering the question, we have to disclose some of the methodologies that we do use.

Senator LUDWIG—At the end perhaps. I do understand the sensitivity in relation to some of these matters but I am trying to find where the line is between when a TI warrant is required and when it is not required and when an ordinary search warrant will do, and what power that will then give you. In your submission you say that the bill will not give the AFP new or greater powers. I remain unconvinced of that.

Federal Agent Lammers—You will know that under a TI warrant the person upon whom we serve a warrant is not notified that there is going to be an intercept. There are considerably more safeguards under the search warrant regime, as Mr Van Dam pointed out earlier, particularly if the search warrant is executed on the premises and the occupant of the premises

is home. There is a whole system and a regime that follows in terms of advising that person that the search is going to be conducted, that he or she will be there while the search happens and while property is removed from the premises, if that is the case. None of that is currently available under the T(I) Act. So the protection under the T(I) Act in terms of advising a person is actually stronger under the search warrant regime.

Going to your question about remote access of information and whether or not technology exists to do that, I am happy to provide you with some examples in camera. But the simple answer is, yes, of course it is possible. In a technological age like this, of course it is possible. You said yourself that you can access your email from anywhere and I think evidence before this committee before alluded to the fact that remote application and remote access is possible. Methodologies involved in doing that, however, are protected.

Mr Van Dam—It is about at what point would a search warrant versus a telephone intercept warrant apply in those circumstances, and it may be possible to discuss those in the context of a practical example in confidence.

Senator LUDWIG—The last area I was interested in was the interaction of the Privacy Act with this area. I take it that you have not had an audit recently in relation to the privacy principles, or have requested one. Have you asked the Acting Privacy Commissioner about some of these issues?

Mr Van Dam—We have not asked the Privacy Commissioner about the impacts of the proposed amendments.

Senator LUDWIG—And the storage and use and how you might ensure third parties' interests are protected.

Mr Van Dam—We have not sought the views of the Privacy Commissioner on that question. As I indicated to you, members of the AFP are obviously obliged under the provisions of the Privacy Act to apply appropriate safeguards and protections to information. Those apply whether or not the information accessed is in a hard copy form or in fact is a derivative from stored communication. As a general principle, AFP officers are subject to privacy provisions in relation to any information that comes into their possession.

Senator LUDWIG—Your submission says—I think I quoted this earlier—this will not give the AFP new or greater powers. Do you still stand by that?

Mr Van Dam—Our belief is that what these amendments do is resolve beyond doubt some ambiguity and that there are no new powers conferred under these provisions.

Senator LUDWIG—So under 3L and the existing powers you can do all of these matters that are the subject of this bill?

Mr Van Dam—That is our belief.

Senator LUDWIG—So the 12-month review, in that instance, would allow you to continue using all these powers that you say you have under the bill in any event and are just confirmed by the bill?

Mr Van Dam—Over the course of the review, it removes the ambiguity about what we believe those powers are. But, as I indicated, it will also give us an opportunity to have a look

in detail at the impacts of new technology and any practical issues that have emerged, historically and over the course of that 12 months, in terms of the application of all of these provisions covering telephone interception and search warrant as it relates to stored communication. It seems to be a very sensible vehicle where these matters can be brought forward.

CHAIR—Before we take the committee in camera, I want to ask about the safeguards and protections that you referred to in the submission and that you also referred to earlier in relation to IPPs and the Privacy Act. If we are dealing with interceptions under the Telecommunications Act, there are procedures and protections for how that information that is obtained can be retained or kept. What are the protections and procedures which apply to information obtained under this bill?

Mr Van Dam—Broadly speaking, this will come down to our guidelines and arrangements for handling of any evidence, so our normal evidentiary handling protocols and procedures apply to this. As I indicated to Senator Ludwig, our normal practice is that, to the extent that material is not required in the context of a prosecution or for the investigation, we have an obligation to hand that back. To the extent that material is retained that could be evidentiary, we have processes and guidelines around the handling of evidentiary material. So material gleaned under these arrangements is no different to material that is gleaned in the course of any other search warrant activity.

CHAIR—The submission states that the bill is required as a priority in order for the Australian Federal Police to meet urgent operational needs. Why weren't they urgent operational needs in February?

Mr Van Dam—I think what we are saying is that these operational needs are real time. We have a need to be able to access this type of information in order to effect our operational activity, and that is a need that exists now. To the extent that the ambiguities have been highlighted and that we see this legislation as clarifying those ambiguities or removing them from ambiguity, we think it is important so that we can get on and undertake that normal activity. The longer that ambiguity remains the more potentially damaging that is to our operational activities.

CHAIR—But it was not a problem in February?

Mr Van Dam—It was a problem to the extent that the ambiguity was—

CHAIR—You did not really answer the question, with respect, Mr Van Dam.

Mr Van Dam—It was a problem in February—as we put in our last submission, we believed that we had the authority to undertake the activities that are contemplated by these amendments. There is conflicting advice, and I think it has created an urgent need.

CHAIR—I am just trying to find a reference in our previous report to a matter I wanted to raise with you, but I will raise it without finding it. One of the priorities which the previous bill had and discussed was an endeavour to address concerns about privacy issues in particular; but this bill suggests an even broader exclusion should operate to give access to communications before they might have been read by the intended recipient—just under a search warrant. So I go back to the fact that there is no specific requirement in that ordinary

search warrant process generally to consider privacy issues. Given that we are going to have a review within 12 months or over 12 months, wouldn't it be more logical to consider these issues in the process of that review? We seem to have walked away from an effort to look after privacy to at least some degree to virtually none.

Mr Van Dam—There are two dimensions to that, I think, and they go back to the earlier point: would the AFP support not moving ahead with these amendments to allow the review to take place? To the extent that that is the question, our answer is that we believe it is imperative that we get clarity around our capacity to undertake that investigative activity, so to defer that would be problematic. To the extent that stored emails are in our view generally in the nature of 'other written communication' the search warrant provisions at the moment allow us to access post office boxes, for example, and retrieve material that may not be opened. The courts ultimately will provide a level of protection as to the extent to which any of that material can be relied on as proof, because the question will remain: did the person open it, understand it and respond to it? So to that extent we do not see these provisions as giving us any power in the electronic context—around accessing stored communication—than they would in the context of hard copy communication.

Federal Agent Weldon—If we went down that track, in the interim we would not be able to expeditiously access—in some situations, access at all—voicemail and emails held remotely where we reasonably suspected that they were related to the commission of a Commonwealth indictable offence, and that would place some evidence at risk of being lost. Our concern is that we would not be able to effectively fulfil our investigative capacity. As for the privacy concerns, as we iterated earlier we are still obliged to comply with the Privacy Act and the Australian Federal Police secrecy provisions under the Australian Federal Police Act, and we may be subject to disciplinary or criminal action if we fail to comply with those.

Senator LUDWIG—I was curious; it seems that you support the review of this legislation ensuing in 12 months time. That is right, isn't it?

Mr Van Dam—The review over 12 months.

Senator LUDWIG—In your view, what is left unresolved that the review would focus on?

Mr Van Dam—In supporting the review we are acknowledging that technology has changed considerably over the past several years and will continue to change. To the extent that the telephone intercept legislation has been in place for some time and these types of amendments emerge, our view is that it is appropriate to take the opportunity to look at the emerging technology and, in our context, the utilisation of technology by criminals and then come to a view about whether the entire framework and approach is going to be sufficient and robust enough to lay a legislative foundation for the future. So to the extent that we support the review there is an opportunity to have a fundamental look at where technology might take this.

Senator LUDWIG—But, in terms of a review resolving any ambiguity between your view of the telecommunications interception power as it is now and what this bill will do, there will not be an ambiguity anymore if this bill is passed, in your view.

Mr Van Dam—We believe that this clarifies that ambiguity.

Senator LUDWIG—Are there any other ambiguities in the TI interception area that you say exists? I will confine you to this area.

Mr Van Dam—When you say 'this area', you mean—

Senator LUDWIG—Stored emails, communications, SMS, telephone, voiceover and Internet.

Mr Van Dam—For the purposes of AFP operations, we believe this clarifies it to the point where we can expeditiously attend to our activity by utilising the appropriate legislative regimes.

CHAIR—This committee has considered this piece of legislation in various incarnations, a number of other pieces of legislation on the same lines and then, over and above that, a broad range of legislation that has provided increased powers of different sorts to the Australian Federal Police in a range of contexts. I must say that we have never been asked to consider a piece of legislation that removes powers from the Australian Federal Police, at least in the time I have been in this position. It strikes me as passing curious that in giving a 12-month power and then purporting to have a review at the end of that there is any pretence at all that it might even move backwards. I see providing the power now as providing a power that probably ends up set in concrete. Is that a reasonable observation?

Mr Van Dam—To the extent that we believe the power clarifies, we would be happy to see the power in place. The question of whether or not there is a 12-month sunset is not one for the AFP. It is ultimately a policy consideration.

CHAIR—That answers my question better than I could possibly have imagined. Thank you.

Evidence was then taken in camera, but later resumed in public—

[11.27 a.m.]

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

HOLLAND, Mr Keith Colin, Acting First Assistant Secretary, Information and Security Law Division, Attorney-General's Department

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

CHAIR—Welcome. We do not have a submission from the department. I invite you to make a brief opening statement, at the conclusion of which we will go to questions.

Mr Ford—I was not intending to make an opening statement. We will of course assist the committee as much as we can in answering questions, but there is one matter that I should clarify. That is that one of the functions of the Solicitor-General, as the second law officer of the Crown, is to resolve differences of legal advice that may emerge within the Commonwealth. He has done that in this case, and in our supplementary submission to the committee we provided details of that opinion. The department bases its advice to agencies on the Solicitor-General's opinion, and the difference between the two bills that have been referred to this morning is in essence this: the first bill reflected the existing legal position as the Solicitor-General advised it, while the second bill makes changes and those changes reflect government policies. The Attorney-General, in his second reading speech, referred to the recommendations of this committee and said that the advancement of the bill should be:

... deferred pending resolution of differing interpretations of the current operation of the interception regime.

He said:

That resolution has now been achieved.

It is clear that he was talking about legal issues. He went on to say:

Thus this bill adequately addresses the operational concerns raised by the Australian Federal Police in relation to access to stored communications.

So any policy differences that may or may not have existed between the department and the AFP are, I submit, irrelevant, because we have no different policy position from that of the government. The resolution of the legal issues included the point that section 3L is simply not available in relation to any communication that is protected by the Telecommunications (Interception) Act.

CHAIR—There are obviously some tradespeople in the roof above the committee room, which made it quite hard to hear the conclusion of what you were saying.

Senator LUDWIG—They are looking for a round, clear, perspex viewing window.

CHAIR—We will try and continue and see what happens in relation to that. Thank you very much. I think I caught most of what you were saying. You said that in the Attorney-General's second reading speech he had indicated that the legal resolution has been achieved, so in the government's view the bill addressed the operational concerns that were previously

raised. The bill itself does introduce some new aspects which the committee had not previously considered, so these certainly remain on foot, even if we agree that the other has been addressed.

Senator LUDWIG—Wouldn't it have been easier to simply say, and perhaps I open it up for a discussion, that in relation to a bill or an amendment to this area 3L is excluded or included in terms of what the AFP say their powers are, rather than rework the telecommunications interception legislation—in other words, that 3L applies in the way that the AFP say it does, giving certainty to 3L rather than dealing with this area?

Mr Ford—I suppose that would be one way of doing it, but the decision is instead focused on whether the scope of the T(I) Act should be changed from what we currently believe it to be and then to allow other laws—not just 3L, but other laws in general—to have their full operation, having removed stored communications from the coverage of this act.

Senator LUDWIG—Yes, because it could have simply said, 'Clarify that nothing in the act affects the operation of 3L,' which would have been a simpler way. What other areas, then, do you say outside of 3L? It seems to be, and I think you heard, that the AFP rely on 3L. They did not seem to allude to any other power, so what other power are you talking about?

Mr Ford—I invite Ms Tearne to address that.

Ms Tearne—Certainly a wide range of powers would be available. Essentially what the amendments do in excluding stored communications from the protection of prohibition against interception is to make those communications accessible by such other powers as may be appropriate in the circumstances, and that will vary across the agencies. The AFP have made reference to 3L, which is a specific search warrant power that they have under the Crimes Act. I believe ASIC mentioned this morning their own compulsion powers and search warrant powers. A number of other agencies have powers to compel the handover of information in certain circumstances. So there are a range of mechanisms through which this information will now be accessible to the extent that it is no longer precluded by the requirement for a telecommunications interception warrant.

Senator LUDWIG—So it would significantly increase the power available to a range of law enforcement agencies and other agencies including ASIC in their ability to access both read and unread emails stored on ISPs?

Ms Tearne—Yes, it would broaden the range of information that is accessible under those powers that they already have.

Senator LUDWIG—They do not have that power, as I understand it from ASIC's submission.

Ms Tearne—They do not, to the extent that access to those communications is currently precluded by the Telecommunications (Interception) Act.

Senator LUDWIG—To be fair, they say it is a bit grey in respect of that area—but continue, please.

Ms Tearne—At the moment the Telecommunications (Interception) Act precludes ASIC and a variety of other agencies that do not have telecommunications interception powers from accessing those communications that are in their passage over the telecommunications

system. These amendments will specifically exclude those communications that have been stored from the operation of that prohibition. So those particular communications will then be accessible through the range of other powers that were not capable of requiring production of that information because a specific requirement for a telecommunication interception warrant overlaid that process and precluded access under a search warrant, for example.

Mr Ford—I will briefly add to that. The thinking behind that is that the interception act is necessarily focused on certain particular agencies: it is basically only police agencies and so on that can carry out interceptions. Other agencies which have an interest in collecting electronic information in one form or another are limited if they are not intercepting agencies. So, if you narrow the scope of the interception act, it allows room for those agencies' powers to operate according to their terms.

Senator LUDWIG—It a significant expansion of the ability to access stored communication without a telecommunications interception warrant across both law enforcement and other agencies, isn't it?

Mr Ford—Yes.

Senator LUDWIG—You then say that in 12 months you will have a review. So once the horse has bolted you will then review to see where the horse has gone. I am not sure of the utility of a review after 12 months once you have enlarged the power the way you say you have.

Mr Ford—The Attorney-General referred to the review in his second reading speech, and I probably cannot add to that with any real substance.

Senator LUDWIG—So you do not know when the review would be held or what the terms would be.

Mr Ford—He made it clear that it is to be over the 12-month period.

Senator LUDWIG—Yes, I know. Starting from when?

Mr Ford—Those details have not been worked out yet.

Senator LUDWIG—Terms of reference?

Mr Ford—They have not been worked out yet. They would need to be discussed with the Attorney.

Senator LUDWIG—You may recall that last time there was a fair bit of interest in what the definition of interception was in the previous 2004 bill—the extension to include reading and reviewing. That was removed altogether from the current bill. Why was that?

Ms Tearne—After the committee's comments and recommendations in relation to the previous bill, the government took those comments into consideration. My understanding is that the intention is to progress the current policy, which is to exclude stored communications from the prohibition against interception.

Senator LUDWIG—The reason I ask is that the EM to the previous 2004 bill said the amendments:

... extend the protection afforded to communications in their passage over the telecommunications system to include protection from reading or viewing those communications. This extension addresses

advances in technology which have resulted in many telecommunications now taking the form of written words, such as email, or even images and to which the concept of listening is not directly applicable.

That is a quote about why reading and viewing were necessary as part of the bill. So why was it necessary to remove those specific words? Some submissions, like Electronic Frontiers', spoke about reading and viewing by telecommunication company employees and expressed concern that the amendments would allow telecommunications carriers and their employees, in their capacity as network owners or administrators, to freely access customers' electronic communications passing over their Internet once they met the definition of stored communications. Do you have a view about that?

Ms Tearne—I am not sure if I entirely understand the question, but I offer the comment that, by excluding stored communications from the protections of the interceptions regime, the definition of interception in relation to those communications then becomes largely irrelevant to the extent that any access to those communications will no longer be prohibited. It is therefore not necessary to—

Senator LUDWIG—I think that is right. What that means is that an ISP's employees can access stored communication on an ISP server. Is that right?

Ms Tearne—Stored communications will no longer be protected by the interception act. That is correct.

Senator LUDWIG—Is that a policy decision that has been made by government to allow that?

Mr Ford—Yes.

Senator LUDWIG—What privacy concerns were taken into consideration?

Mr Ford—Privacy concerns were taken into account. Some of those were covered this morning in your questioning of the Acting Privacy Commissioner.

Senator LUDWIG—I am not sure that you retained him to do any work in this area, though.

Mr Ford—The timing for the introduction—

Senator LUDWIG—You consulted with him for two days prior—would you call that consulting, Mr Holland?

Mr Ford—The timing was very tight. We were required to move within a very tight time frame in order to meet the deadlines for getting bills into the parliament and so on, so it just was not possible to give more time—

Senator LUDWIG—We are still here.

Mr Ford—Yes. Could I just—

CHAIR—When was this?

Senator LUDWIG—That was February.

Mr Ford—I see. I thought you were talking about this particular bill that has just been introduced.

Senator LUDWIG—But it does not preclude you from going back and talking to the Acting Privacy Commissioner about that bill and this bill, because you are not certain what is going to happen. I am not certain what is going to happen.

Mr Ford—Certainly. That consultation does take place—I do not have the details—from time to time.

Senator LUDWIG—There has been no continuing communication or consultation about this, has there?

Mr Ford—Since this was introduced?

Ms Tearne—No. In the context of the current amendments it was not possible, in the circumstances, to conduct the kind of consultation in which the department would usually engage in developing this interception legislation.

Senator LUDWIG—I would be careful about how you use 'usually engage' with this committee. Our experience with Attorney-General's—the chair might want to add to this—or my experience, if I put it that way, is that Attorney-General's has not been particularly good about consulting agencies on legislation that is going to be introduced and brought before this committee. What we have discovered is that, if you do, some of these concerns are met before the committee gets to the point of asking about them, which seems an inappropriate way of dealing with it, where we then have to start asking about this range of issues that otherwise would have been dealt with prior to getting here. Maybe you could take that back to your peers—maybe you could pass this conversation onto Mr McDonald as well.

Mr Ford—I will. Perhaps I will just say in relation to—

Senator LUDWIG—Tell him we are still disappointed with him!

CHAIR—It is uncharitable in the context of this committee hearing, Senator Ludwig!

Senator LUDWIG—Going back to the issue of ISPs accessing stored communication, there is no longer a prohibition in respect of employees' communications. As such, do you say the ordinary privacy principles then would apply to the company as to how they deal with that information?

Mr Ford—The privacy principles that would apply to the ISPs are the national privacy principles which Mr Pilgrim referred to before—NPP 2.

Senator LUDWIG—Are you aware of whether procedures and protections as to how information is obtained—through ordinary search warrants for stored communications or the like—would be maintained by law enforcement agencies or by other agencies that now can access that information?

Ms Tearne—I certainly would not be able to comment in detail on the whole range of mechanisms that could now be used to access information, but essentially the effect of the amendments is to allow those communications to be accessible under such other forms of lawful access as may be appropriate in the circumstances. Some of those, as I believe the AFP and ASIC intimated this morning, are the subject of particular arrangements with their own agencies, but I could not provide a comment on behalf of the whole range of powers that would be about.

Senator LUDWIG—How many agencies are there? How many agencies would then have access to stored communications on ISPs? For argument's sake, ASIC say they effectively use an order for information. What other agencies would then be able to access stored communications?

Ms Tearne—I do not think I could provide you with a total number. The amendments do not distinguish between which agencies would have access and which agencies would not. What they do is generally remove them from the prohibition against interception, and so those agencies that would otherwise have access to information as a general proposition would thereby be able to use those powers in relation to stored communications. There would obviously be quite a number of law enforcement agencies and those others that have compulsive powers.

Senator LUDWIG—So how would those agencies, or the public generally, know that the law has changed significantly and that the protections that were afforded are no longer afforded?

Ms Tearne—To the extent that the legislation—

Senator LUDWIG—They would guess, would they? I do not want to put words in your mouth. It is a legitimate question: how would they know?

Ms Tearne—If passed, the legislation would be a matter of public record; it has certainly been the subject of significant comment. The department has a role in advising agencies, and it responds to queries on the current state of the law from a wide range of fora. We participate in a range of fora at which we provide regular updates on the way the interception legislation operates. I could not point to a particular mechanism that would mean the general public at large would be aware of the changes, but there are certainly a range of fora and mechanisms that the department engages in to ensure that information is disseminated, to the extent that that is possible.

Senator LUDWIG—Section 7(3A) of the bill excludes the definition of stored communication, which is communication 'stored on a highly transitory basis as an integral function of the technology used in its transmission'. I am not sure what that means—but that does not surprise me. Can you tell me what that means?

Ms Tearne—What that particular provision does is ensure that communications—

Senator LUDWIG—I want to know what it means. We will get to what it does shortly.

Ms Tearne—I believe the explanatory memorandum provides some comment on 'highly transitory'.

Senator LUDWIG—I am happy for you to tell me what that means as well.

Ms Tearne—It means very brief, very short. I think the explanatory memorandum gives the example, in some circumstances, of even a fraction of a second. It refers to storage on a very temporary basis.

Senator LUDWIG—Can you give an example of that?

Ms Tearne—The very specific example is 'voice over Internet protocol'. To the user, VOIP communications function like standard telephony, but the communication is transmitted

via IP packets. Those packets are stored for a fraction of a second while the computer equipment that is responsible for transmitting the communication resolves the path of the communication and determines where it is to go. It holds the communication for a very brief second and passes it on. The particular provision in the bill is designed to ensure that that very brief storage does not render those communications stored communications for the purposes of the exception to the prohibition. Notwithstanding that very brief storage, those communications will continue to be protected by the prohibition against interception.

Senator LUDWIG—What about chat rooms? Is that stored communication or is it 'stored on a highly transitory basis as an integral function of the technology used in its transmission'?

Ms Tearne—Communications can be stored at a number of stages in the course of their transmission. My understanding is that the course of a chat room communication could involve both types of storage. Chat room communications can be stored on a basis that would be sufficient to have them amount to stored communications. Another example of highly transitory storage is a type of buffering that occurs for a small moment while communications are successfully transmitted. That occurs not only in chat room communications but also in email and some mobile phone communications. The very brief storage that is necessary as a function of getting the communication through—and, again, that is usually a matter of seconds or even a fraction thereof—does not render the communication a stored communication at that point. But chat room communications can be stored on the user's computer in other records. A record of that session can be created, and that record would be a stored communication.

Senator LUDWIG—In relation to SMS messages or emails, what in your view would be included in the definition of a stored communication and what would be excluded?

Ms Tearne—The definition of a stored communication includes anything that is stored on equipment. Therefore it does not include those communications that are not at a particular time stored but which are in fact moving—hence the reference to 'live and real-time transmissions' in the explanatory material and other documents relating to this bill. Anything that is sitting still and is stored on equipment, bar that storage which is very brief and necessary as a function of the transmission of the communication, would be a stored communication. An SMS message on a telephone is a stored communication. A voice mail residing on the equipment of a carriage service provider who is providing a voice mail service is also a stored communication.

Senator LUDWIG—And if they use a camera and a computer that also carries voice, that would not then be stored, but if they stored it, it would be stored? If they used a remote camera—if they set up a webcam—is that stored communication if it is then captured?

Ms Tearne—A communication that is sitting somewhere and is stored—

Senator LUDWIG—A lot of the web cameras also have microphones attached to them.

Ms Tearne—The live transmission of communications backwards and forwards between users and over the Internet remains protected while a communication is transiting between users. Any record that is created and kept and is in storage, be that at the end of a communication or indeed in transit, anything that is stored—someone else said anything that is sitting still—is a stored communication.

Senator LUDWIG—Have you had discussions with the AFP about whether this bill resolves all the issues that they may otherwise have had in relation to stored communication and access of emails and SMSs?

Ms Tearne—We have had discussions with the AFP, yes. I understand that this bill addresses their concerns.

CHAIR—Thank you very much. If there are any further questions, we will take those up with the department on notice, with your agreement. That covers most of the issues which have been canvassed with preceding witnesses this morning. On behalf of the committee, thank you very much for your assistance.

I thank all of the witnesses who had given evidence to the committee today in this hearing on the provisions of the Telecommunications (Interception) Amendment (Stored Communication) Bill 2004 and declare this meeting of the Senate Legal and Constitutional Legislation Committee adjourned.

Committee adjourned at 11.51 a.m.