



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE

Reference: Cybercrime Bill 2001

THURSDAY, 19 JULY 2001

SYDNEY

BY AUTHORITY OF THE SENATE

WITNESSES

ARGY, Mr Philip, Vice President, Australian Computer Society	13
ATKINS, Mr Michael Francis Charles, Special Adviser Law Reform, Australian Federal Police.....	23
BOXALL, Mr Jonathan James, Acting Team Leader, NII Incidence Analysis and Response Team, Australian Federal Police	23
CHIDGEY, Ms Sarah Jane, Legal Officer, Criminal Law Branch, Attorney-General’s Department.....	33
McDONALD, Mr Geoffrey Angus, Assistant Secretary, Criminal Law Branch, Attorney-General’s Department.....	33
McDONALD, Mr Robert Richard, National Director, National Crime Authority	1
ORLOWSKI, Mr Stephen Robert, Consultant, Attorney-General’s Department	33
TEBBET, Mr Robert John, National Manager, Technical Support and Physical Surveillance, National Crime Authority	1
WALTERS, Mr Mark Adrian, Acting Director, Investigations and Technical Operations, Australian Federal Police.....	23

SENATE
LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
Thursday, 19 July 2001

Members: Senator Payne (*Chair*), Senators Coonan, Cooney, Greig, Mason and McKiernan

Participating members: Senators Abetz, Bartlett, Bolkus, Brown, Calvert, Chapman, Crane, Eggleston, Faulkner, Ferguson, Ferris, Gibson, Harradine, Knowles, Lightfoot, McGauran, Stott Despoja, Tchen, Tierney and Watson

Senators in attendance: Senators Coonan, Cooney, Ludwig, McKiernan and Payne

Terms of reference for the inquiry:

Cybercrime Bill 2001.

Committee met at 11.30 a.m.

McDONALD, Mr Robert Richard, National Director, National Crime Authority

TEBBET, Mr Robert John, National Manager, Technical Support and Physical Surveillance, National Crime Authority

CHAIR—The [Cybercrime Bill 2001](#), as stated in the explanatory memorandum, will amend a number of acts, including the Criminal Code Act 1995 by adding a new part, 10.7, which contains new updated computer offences based on the January 2001 model criminal code damage and computer offences report, developed through Commonwealth, state and territory cooperation as a model for national consistency. The bill will also enhance investigation powers relating to the search and seizure of electronically stored data by amendments to the Crimes Act 1914 and the Customs Act 1901.

The Senate referred the bill to this committee on 28 June 2001 for inquiry and report by 21 August this year. The committee advertised the inquiry on 7 and 8 July 2001 in the *Australian* newspaper. The closing date for submissions to this inquiry is, in fact, tomorrow, 20 July 2001. However, the committee has agreed to hold this preliminary public hearing to advance our consideration of the bill. I call the committee order and welcome Mr Robert McDonald and Mr Robert Tebbet from the National Crime Authority. The National Crime Authority has lodged a submission, which the committee has numbered 2. Are there any amendments or alterations you wish to make to that submission?

Mr R. McDonald—No, not at this stage.

CHAIR—Thank you very much for lodging that submission. As you know, it came in just this morning and the committee has not had a chance to consider it in any detail, but we are very thankful to the NCA for providing us with that. I would also note the committee's grateful thanks to the NCA for shifting the time of their appearance before the committee. I am sure it has not been a convenient change for you but we are very grateful for your assistance, because other witnesses have been unable to join us at the appropriate time. Mr McDonald and Mr Tebbet, would you like to make a short opening statement and, at the conclusion of that, I will seek questions from members of the committee. I note for the record that you will not be asked about your view on matters of policy or reasons for policy

decisions and that, if it is necessary, we will, of course, give you the opportunity to refer those matters to the appropriate minister. Mr McDonald, do you have an opening statement?

Mr R. McDonald—Thank you, Madam Chair. Ladies and gentlemen, in addition to the submission that I believe you all have, I would like to say that we live in an age where technology is rapidly changing, with new equipment and facilities constantly coming on to the market. In summary, these new technologies have increased the opportunities for organised crime and have lessened many of the risks of detection. This is significant in Australia, which boasts a high rate of adoption of modern technologies, as instanced by the use of mobile telephones and the Internet for communication. We see the aim of the bill as ensuring that law enforcement keeps pace with technological developments and new types of computer crimes, both where technology itself is subject to the crimes and where crimes are committed using the new technologies.

The NCA sees this as part of a continuing process. For instance, the NCA is seeking to develop a cyberforensic capacity to enable it to investigate criminal activities involving the use of computers. Accordingly, the NCA supports the bill as an important first step to facilitating law enforcement and in maintaining the capacity to detect, investigate and prevent criminal activity on behalf of the community. This is an important step towards the international harmonisation of laws, and the NCA particularly supports the proposed new powers that will enable effective searches of computers and other electronic equipment. This will assist law enforcement agencies to circumvent encryption used by criminal syndicates by obtaining direct access to original messages and documents.

CHAIR—Thank you very much, Mr McDonald. Mr Tebbet, do you wish to add anything to that?

Mr Tebbet—No, I have nothing further to add.

Senator McKIERNAN—The NCA supports the new powers of law enforcement; those new powers are pretty dramatic, are they not?

Mr R. McDonald—This is a new type of crime and I think you certainly need new powers to be able to counter the criminal attack that can eventuate from this type of technology.

Senator McKIERNAN—The networking of computers is something that is around now. If there is a suspicion of an offence being committed in one place and a computer is networked to the computer in the facility where the suspected crime is being committed, can the other device in another location also be examined and, if there is data contained in that, can it be copied and indeed removed from that particular premises?

Mr R. McDonald—Yes, that is my understanding of the legislation, but it has got to be in relation to a criminal offence. In other words, you would not be using or taking information that is not related to what you are investigating, as I understand it.

Senator McKIERNAN—Yes, but you will not know what is related to it until you look at it, will you?

Mr R. McDonald—That is very much the same now. If I were to take a search warrant and go into someone's house or, say, go into an accountant's office or a solicitor's office while investigating a major fraud, there may be documents caught up with other documents that I would need to take away and examine in the cold, hard light of day to be able to ascertain whether or not they form evidence in relation to the matter we are investigating. The same would happen in relation to a computer. If it is on a hard disk somewhere, you do not really know all the time that the information is relevant to the matter that you are investigating until you go through it and are able to look at it properly.

Senator McKIERNAN—I think that is a useful analogy that you used, Mr McDonald, but, as I understand the bill, were you to go in with a search warrant and look in a filing cabinet for documents, the search warrant would not entitle you to take away the filing cabinet in bulk. It would entitle you to search through the filing cabinet to see what was relevant to the inquiry; whereas, the provisions of this bill will indeed allow the law enforcement officers to take away what is on the hard disk of the computer, perhaps even in another location.

Mr R. McDonald—With our powers at the moment, it is possible for us to take that complete filing cabinet if there are documents in there that relate to the offence, and you may have other information caught up in amongst those documents that would not form part of the evidence in relation to the matter that you are investigating. I have done that with the many investigations I have been involved in where you look through, you see material that is relevant to the offence that you are investigating, you take it away out of the war zone—if I can call it that—and you have got the time to go through it and look at each separate document. You will soon find that many of those documents do not form evidence to the matter and should be returned.

Senator McKIERNAN—You say you did look through the documents to see if they were relevant to your inquiry and then you took them away but, in the course of doing that, documents that were not relevant to your inquiry would be left in the war zone, as you describe it.

Mr R. McDonald—No. I was saying that you would take it all. Often when you are executing search warrants there is a lot of activity and a lot of emotion involved, particularly if you are impinging on someone's privacy in their own home or if you have walked into business premises. You cannot really make the full judgment there and then at the time. You need time to go away and be able to go through those files to identify what you would seize as evidence and identify those documents that you would return to the individual concerned.

Senator McKIERNAN—So your argument now is that the search warrant just covers the filing cabinet, as it were?

Mr R. McDonald—Yes. If in each drawer and in each one of those documents there was a piece of paper that was relevant to the offence that you were investigating and in behind that or mixed up with that there are other papers that are not relevant, yes, you could take all those documents. You believe at that stage that it is going to provide evidence or assistance to the investigation; you have a suspicion.

Senator McKIERNAN—How does that operate with a computer? You would be dealing, as it were, with a compactus filing system rather than just a filing cabinet. I am trying to put it in language that I would understand. If you want to interpret it slightly differently, please do so by all means.

Mr R. McDonald—I am no computer expert. I have come from a law enforcement background, and I would apply the same principles if I were a player looking at a search warrant. Someone has to have the ability and capacity to open up those files, and it may take an expert to do that, whereas you would require the investigator who is in charge of the investigation to go through and analyse whether what is contained within those files is relevant to the offences they are investigating. It is very similar to a document. You would have to get into it, open it up and look at it before you could make that judgment.

Senator McKIERNAN—So only documents are relevant to the investigation? I thought this bill went slightly further than that and gave the right to copy what was on that other computer or to even take away the hard disk.

Mr R. McDonald—That is my understanding too. You would not be able to use that material if it did not form evidence for the offence that you were investigating or that you would be charging with.

Senator McKIERNAN—But you do not know what is relevant until you look at it. The bill gives the law enforcement officers an entitlement to either take the hard disk away or copy what is on the hard disk. Let's face it: in this 72-hour period you will not be able to look at each and every document that would be contained in a computer.

Mr Tebbet—The difficulty we have is the massive amounts of data that a computer or a network could hold; there is just so much of that. The investigators would be certainly trying to focus on the areas that would be of interest to them to further the investigation. It would take a massive amount of time—hours—to go through it all. Until such time as it can be examined or some sort of technology can be put across that information to try to solicit out the type of evidence that we would need, I do not see that there is any way other than being able to actually have the opportunity to view what is available.

CHAIR—I have one question on this subject. As I said, we are treating this very much as a briefing environment in a lot of ways. What privacy protections are in place for other people whose material may be on the hard disk for, in the normal course of events, the work that the NCA, the AFP and so on undertake in this context? Will privacy provisions, assuming they exist, be implemented in these changes?

Mr R. McDonald—Going back to the original analogy I made with the search warrant, you would have to make application for a warrant to be able to do it. You must go before a judicial officer, a magistrate, and be able to satisfy that magistrate, on the material that you are placing before him, that you have grounds to look at that material. If amongst that material there are files that quite obviously have no relation to the investigation and belong to someone else or have no material substance to the investigation that you are investigating, you just do not touch it.

CHAIR—Is that a formal structure? Are there privacy provisions which are incorporated in some formal advice to investigative officers?

Mr R. McDonald—Yes, there are also departmental procedures surrounding the execution of search warrants and so forth. Also, in the law itself you must have suspicion about that document as to where you go. I understand where the senator is coming from in relation to having to take this massive amount of data, but in that environment you virtually have to be able to take it away to open it up and look at it; you do not have that physical bit of paper in front of you.

CHAIR—Are those procedures amended to take into account changes in technology like the sorts of things we are talking about now? Are they updated regularly? Are officers appropriately trained to deal with them?

Mr R. McDonald—They are updated on a reasonably regular basis, as I understand it. Whether or not the particular procedure in my organisation is encompassing this, I am not sure. I could not say yes or no.

CHAIR—Perhaps you could check on that for us.

Mr R. McDonald—Yes, I will.

CHAIR—Thank you. I am sorry to have interrupted, Senator McKiernan.

Senator McKIERNAN—That is fine. You said in response to Senator Payne that, if the documents are not relevant, you will not touch them but, in actual fact, you have touched

them. You have actually either physically removed them from the premises or indeed copied them. You have touched them

Mr R. McDonald—Yes. But once you are able to make that proper judgment they are returned. If they are of no relevance they are returned to the owner of the property.

Senator McKIERNAN—So the privacy protection provisions are actually set to one side with regard to this in the investigation of a crime. When I made my opening comments about it being a dramatic extension of the law enforcement powers we talked about networked computers. If a crime is suspected of being committed in one place but, because that computer in that physical establishment is networked to another computer in another location, that other computer can also be accessed and its contents copied by a law enforcement body. Would that same search warrant that would apply to the first instance cover the networked computer in a secondary location?

Mr R. McDonald—Do you mean under the new act?

Senator McKIERNAN—The new amendment act.

Mr R. McDonald—Yes, I believe so on my initial reading of it. The Attorney-General's Department might be in a better position to advise on the legalities of that more so than I. I have only briefly skimmed some of this material before coming before this committee. I hasten to add that we must have suspicion of what is in there. When you go and make application for a search warrant you specify in it the types of files and documents you are looking for, and on a quick glance you can practically tell whether that file is going to be relevant or not—whether that alleviates some of the fears in that area, I do not know.

Senator McKIERNAN—Neither do I.

Mr Tebbet—Also, it is a bit like the other privacy intrusive tools of investigation that are available to law enforcement—for example, telephone intercept and the use of listening devices. Telephone conversations are intercepted but only those that are of evidentiary value are ever used. There are strict guidelines as to how we must behave and use that type of thing. It is the same with the listening devices. I am sure there will be guidelines and processes put in place to ensure that these things are managed the same way.

Senator McKIERNAN—Are they? That is the point: we have got the bill.

Mr Tebbet—There are certainly guidelines and processes in place for the execution of search warrants. I am sure they will be in place with respect to this. I would be sure that those guidelines that are in place would be amended to reflect our responsibilities to this legislation as well.

Senator McKIERNAN—I guess the NCA's brief would be your first priority. In your brief would not be the protection of privacy. Your brief is the investigation of a criminal offence. I am looking at your powers and the execution of your search warrant. In a theoretical instance, if we had a crime against the Commonwealth being committed out of a Commonwealth office and that Commonwealth office was linked to the parliamentary computer then, theoretically, every computer held by every senator and every member of parliament could be accessed by the investigating law enforcement authority in order to further investigate the crime if they thought there was a link-up.

Mr R. McDonald—I would be very surprised if that were to happen inasmuch as the information in the search warrant, to grant the search warrant in the first instance, would not permit us to go in and open up files that obviously have no connection to the matter that we were investigating.

CHAIR—You are saying that you are restricted by the nature of the search warrant.

Mr R. McDonald—Yes. The search warrant will have parameters around it and the information has to be grounded, as I say, before a magistrate to be able to get that permission in the first place.

Senator McKIERNAN—But didn't you just tell me a little while ago that the original search warrant would cover a computer that was networked to the computer where the crime was initially suspected of having occurred?

Mr R. McDonald—Could you say that again, please?

Senator McKIERNAN—The downstream networking—I am not a computer expert either.

Senator LUDWIG—For argument's sake, if you put material in a folder on the network and not on your hard drive, it is then on the server so it is not necessarily connected to person A's workplace. The server could be remotely located in Canberra and person A, the person under investigation, could be in Brisbane. He or she puts the relevant material on the server, which is remote in Canberra, in a file called 'X', labelled 'Do not open because it has got nothing to do with you or anyone else.' To investigate that person A, you look on their hard drive C and there is nothing there. You then have to go into the server to look further. You have to look at all of the server, because the person A could place their files in any location and anywhere on the server. In fact, if they have got authorisation under the system's administrator, they could place it on someone else's hard drive in another location, anyway.

Mr Tebbet—In those sort of situations, certainly the investigating body would be seeking the assistance of the management to facilitate the search, and seeking some guidance from their IT people so that we would not trip over other people's business that we should look at. Guidance would certainly be sought from an IT systems administrator in those sort of situations. There would be so much data and so much information the investigators would not even know what to do with it or where to start, so we would have to seek guidance. I think there are some provisions in there where people are obliged to assist.

Senator LUDWIG—What would the search warrant cover? Again assume person A decides to hold this data that you are seeking to find. They would put it in places where it would be difficult to find, I would imagine, and they would put it in places remote from them—not on their hard drive—and either under encrypted files or alternatively under different names on other people's hard drives or other people's servers in remote locations.

Mr R. McDonald—In drafting or laying the information to get the search warrant in the first place, you narrow the parameters down exactly to what you are looking for on the offence that has been committed. For someone to go and take a file out of, say, their C drive and hide it away in someone else's directory, there would have to be some lead for us to know that they had done that. Through the nature of the investigation we would know exactly what we are looking for. If that lead was there to take us into that other directory, we would pretty well know the file we were looking for was hidden away in there, I would imagine. Other people with more technical nous in this area may be able to answer the question far better than I, also with regard to the technicalities of going into the directories. I do not profess to have any technical expertise in that area whatsoever.

Senator McKIERNAN—A computer is not defined in the bill. There is no definition of what a computer is. It was a recommendation that that be so—but it is going to have to be defined in a court of law somewhere, isn't it? Is it not a weakness in the bill that there is no definition of what a computer is?

Mr R. McDonald—I don't agree. To be quite honest, I see that in some ways as being a strength, inasmuch as it is fairly hard to define, particularly with the way that technology is advancing. What is a computer? What are we talking about here? Is it something that just stores electronic information? If it could be in an in camera hearing, I could give you an example using cash registers. Is that a computer? Is that what we are talking about? I do not know.

Senator McKIERNAN—We might have to take you up on that option. There was a recommendation that there not be a definition, for those very reasons. However, it is going to have to be defined. It probably will be defined by a judge sitting in court, which will then go to an appeal court, and possibly even later on to a higher court for a definition. Are not we, as legislators, abdicating our role in defining the limits on things rather than handpassing to the judiciary?

CHAIR—Senator McKiernan, do I understand you wish the committee to go in camera?

Senator McKIERNAN—Not at this stage. If I am to further enlighten myself—I can only speak individually—on these matters, it might be an option for the future, when we have had an opportunity of reading the submission from the NCA and after we have heard the evidence from the AFP and the Attorney-General's Department, whom we talk with later. I do have concerns on that matter of what a computer is. For example, is a PalmPilot—which the chair uses all the time—a computer? Similarly, as you say, with cash registers.

Mr R. McDonald—I think we are going to see a growth in that area. It is like what you can do with mobile phones now in sending a short message text and so forth across phones. It is such a growth area that it is going to be very difficult. I understand what you are saying in relation to the law courts. There will be good legal argument in the courts.

Senator MASON—My first question concerns privacy and human rights issues and the issue about the warrant that Senator McKiernan and Senator Ludwig raised. When you draft your warrant, what are you after? You are after electronic data, as I understand it. To find that electronic data, are you having to find it on a particular computer, a particular disk or can that electronic data be found on any server anywhere in the world? If the latter is the case, to discover that particular electronic data you may need to follow that information all around the world—is that right?

Mr R. McDonald—There could be scenarios, particularly with organised crime figures, where you could have someone come into Australia who could be involved in an international drug trafficking syndicate and was using the Internet to send messages. They could have information that is relevant to that investigation stored in a computer back in the United States or in South-East Asia or elsewhere which, if you could identify and knew it was there, you would then have to go through the normal international mutual assistance agreements and everything else to be able to obtain that evidence. We would not be able to do that from Australia, as I understand.

Senator MASON—Many years ago I used to practise as a prosecutor. Search warrants were cast as narrowly as possible, and were usually for a particular place for a particular thing. Here the particular thing could be in any place—is that right?

Mr R. McDonald—It would not be in all cases but it could be in some. You could have material in a number of different computers.

Senator MASON—Isn't that the problem? That is what Senator McKiernan and Senator Ludwig are saying. To go after that particular thing, with telephone lines and so forth, you can actually run through people's privacy anywhere. That is the concern that has been raised.

Mr R. McDonald—Your safeguard is within grounding your search warrant and what you are looking for and narrowing it down. It is the same as what we do with—

Senator MASON—I understand that: you cast it as narrowly as possible. Even so, it might be anywhere. It is not in 1 Smith Street, Newtown; it could be anywhere. Rummaging through computers and files throughout the world—

Mr R. McDonald—Yes.

Mr Tebbett—You would not be able to do that. It would be unlawful. It would be beyond the extent of anyone's authority to be able to do that. You just would not do that. We would be acting unlawfully if we did. We have the Council of Europe Convention on Cyber-crime which is a body that is starting to look at these kinds of issues. I have never been to that forum, but I guess that is what that is about. The issues that you raise are very real ones, but I am quite sure that law enforcement in this country well and truly understands that that is beyond the scope.

Senator MASON—Why is it beyond the scope? Is it because it is beyond the scope of your law enforcement and investigative capacity? Is that the reason? Or is it beyond the scope of extraterritorial legislation?

Mr Tebbett—I think both. But beyond the scope of methodology is probably something that is shortening rapidly and it probably will be available in the fullness of time.

Senator MASON—Can we move to investigation powers, just briefly. Maybe this is a question for the Attorney-General's but, as a matter of interest, do you know the degree to which the Model Criminal Code has been adopted by the states and the territories? That question may be unfair; maybe that is a question for the Attorney-General's.

Mr R. McDonald—I would be much more comfortable for the A-G's to answer that question.

Senator MASON—Okay, that is fine. I raise it because I was briefly involved in that. Do you think our mutual assistance legislation that you mentioned is sufficiently comprehensive to justify confidence that these new powers you seek can be usefully and comprehensively implemented?

Mr R. McDonald—I am not confident. It is something that I have not looked at very closely, but the arrangements that we have around the world at the moment are very good. They may very well be sufficient, but I could not say for certain that they would be sufficient.

Senator MASON—Have you attempted in the past to use legislation operating extraterritorially to investigate cybercrime?

Mr R. McDonald—No, not to my knowledge—unless Bob has any knowledge of that.

Mr Tebbett—No.

Senator MASON—What evidence of the problem of cybercrime have you come across in Australia?

Mr R. McDonald—The type of thing we have been coming across is where this technology is being used to assist organised crime in perpetrating other offences—such as international drug trafficking using the Internet and particularly, again, with mobile telephones and the issue of multiple SIM cards and things of that nature. We have also come across the use of it for fraud. I could give an example in camera in relation to cash registers where technology was used to defraud the Commonwealth. That is another example of it coming across. There are instances where we believe some figures have been using certain

software to facilitate money laundering. We have some intelligence in that area. It is in matters of that nature where we have come across it.

Senator MASON—I am not an expert on this but, already, from what we have heard in evidence this morning in answer to questions from my colleagues the financial capacity of the NCA, the technical capacity of the NCA and the extraterritorial capacity of the legislature are brought into question, aren't they?

Mr R. McDonald—Yes, very much so.

Senator MASON—It is not a criticism; they are extremely difficulty issues.

Mr R. McDonald—They are very relevant issues.

Senator MASON—And this would have come out within about 15 minutes.

Mr R. McDonald—Yes.

Senator MASON—Thank you.

CHAIR—In your submission, which I am skim reading as we go, you make reference to the operation of the AGEC—another of the law enforcement acronyms of which I am rapidly becoming familiar—which is chaired by AUSTRAC. You refer also to two newly established Commonwealth interagency committees working in this area: the E-Security Coordination Group and the Critical Infrastructure Protection Group. At what stage are those groups up to in their work? Would you describe them as being a short way down the road, a long way down the road or having a comprehensive grasp of what is happening?

Mr R. McDonald—To be truthful, I have not been a part of those groups and I am not certain just how far down the road they are. I understand that the first group, the Action Group into the Law Enforcement Implications of Electronic Commerce are making quite good progress in their area. I am sorry, I cannot answer your question on the other two groups. I am prepared to take it on notice, if need be, and come back to you on it.

CHAIR—Yes. We will also be seeing other agencies who can assist us with that process. I will ask them further questions in that area. Do you have any knowledge of the extent to which the proposed legislation diverges from the Model Criminal Code suggestions?

Mr R. McDonald—No, I do not. I have not been sufficiently close to it to be able to answer your question.

CHAIR—That is all right. I will come back to that with the Attorney-General's Department.

Senator LUDWIG—Do you know what http stands for?

Mr R. McDonald—No, I cannot answer that. I know it is a part of computer language.

Senator LUDWIG—That is all right. You qualified your remarks earlier that you were not completely computer familiar in this area, and that raises the question: is there anybody in the NCA who is computer literate and who could have come along today and helped us in relation to cybercrime? I say that because I take it you are not going to investigate these matters. It will be people under your control who are familiar with these new devices, and computers and computer programs that will search. I mean, it will not be a physical search through a server to determine what is or is not of interest to you; you will have some form of program that will search. Is the warrant going to match the program in that sense or is it going to be wider than the program that you use or the information you have to set the program off to search servers and deal with it? The question we have come to is: why didn't you bring someone along who might be more able to assist the committee in that capacity?

Mr R. McDonald—I guess you raise a number of issues there. I am not so sure that it is a program that will be doing the searches as more a reliance on the expertise of the people who will be utilising it.

Senator LUDWIG—Yes, I use that as a physical example, perhaps—but the expertise of the people.

Mr R. McDonald—At this stage—and it is a part of our submission, which, on such short notice, unfortunately arrived only just prior to us—we say in our submission that we are taking three steps. Firstly, we are attempting to get training for investigators to be able to handle this. We do not suggest that at this moment we have the level of expertise we should have. That is one phase of the exercise. The next phase is that we are going to try to get some modest cybercrime investigation expertise into the authority, and we are still in the process of doing that. The third phase is for higher level assistance and so forth. Hopefully, there will be another body, so to speak, with that higher level expertise that we would subscribe to provide that assistance to the National Crime Authority. For technical issues in relation to day-to-day management of computers and so forth—if you want to hear from someone like that—yes, we do have some people who manage our IT infrastructure and so forth within the authority, but we do not have what I would term ‘an expert’ in the investigation of it at this time.

Senator LUDWIG—No, it is not a case of what I wanted to hear from it; it is a case of someone to address the bill itself. A further question needs to be asked as to whether it is a horse and cart issue in the sense that you are saying, as I understand it, that you desire a cybercrime bill to be enacted but you do not have the expertise to use it. You are not suggesting that, are you?

Mr R. McDonald—No, to use a computer, do you mean?

Senator LUDWIG—It seems to me that you are saying, in effect, that the legislation is in front of where you are at now—that is, you do not have people with sufficient expertise and knowledge, or investigators either, to be able to utilise the act. I would have thought that the other way around may have been a better way to go. You could use your existing law to the degree where your experts say, ‘We can’t go any further and we need a particular type of bill such as this.’

Mr R. McDonald—Let me say I am talking about our ability internally within the National Crime Authority. If we had a problem, there is expertise out there. We would look towards other organisations for that expertise and bring them in to assist us—also the private sector. There is expertise out there.

Senator LUDWIG—Have you asked any of your in-house computer specialists or people with computer knowledge or anyone external to your organisation that you might usually draw on to have a look at this bill to see whether it meets your requirements in investigating crime of this nature?

Mr R. McDonald—I have not but I would be very surprised if there had not been consultation. In fact, I believe there has been fairly wide consultation on it.

Senator LUDWIG—You do see my point though.

Mr R. McDonald—Yes.

Senator LUDWIG—At the moment you say that you support the legislation, if that is what you are doing, but you do not know whether it will actually meet the requirements that

you might be deficient in. Or, am I going too far? I would certainly like you to have a look at it and come back and answer that.

Mr R. McDonald—We recognise that we need additional expertise within our organisation to move into the future. We believe that the legislation in the bill will be able to handle this particular problem with technology that is arising, and we support that. There has been fairly wide consultation.

Senator LUDWIG—Has there been wide consultation within your organisation?

Mr R. McDonald—And externally with other agencies as well.

Senator LUDWIG—Has that been channelled through you? Have you had it?

Mr R. McDonald—No, by others within the organisation.

Senator LUDWIG—So you cannot say with any certainty that it has been done or that it has not been done, to your knowledge?

Mr R. McDonald—I do believe it has been done. There has been consultation.

Senator LUDWIG—Has the evidence of that consultation been brought to your attention? Has it been presented to you in a report or been given to you in some fashion, or is it just what you think has occurred?

Mr R. McDonald—It is just what I have picked up in discussions with other people within the organisation.

Senator LUDWIG—So it is hearsay in that sense.

Mr Tebbet—We have investigations running at the moment where there is technology that we need to know about and we need to get into. We use the services of the AFP, which has a fairly good standard of expertise and is able to assist the NCA. It is not only large network computer systems; it is things as common as personal organisers and personal mobile telephones. They are the sorts of things that are used by a lot of the targets we are up against. They are fairly simple things to use but, if there is any sort of encryption on those things, they are a nightmare for the investigator. It is the small, common, everyday thing as well as the larger situations that cause us problems with this type of technology. As I say, fortunately, we have had the assistance of the AFP, and some of the other state jurisdictions have been able to help as well.

Senator LUDWIG—I understand that you have identified the problem but I am not sure whether you have convinced me. Perhaps you may want to take on notice the question of whether the Cybercrime Bill addresses your concerns to the extent that it allows that to occur—that is, you are an investigator to do what they want to do. That is the break in the transmission that I seem to be missing.

Mr Tebbet—It would be nice if it extended a little more but I guess we need to start somewhere.

Senator McKIERNAN—I have not read your submission as yet, but I would have an expectation that the NCA would be a strong supporter of this legislation and be one of the driving forces behind the legislation. The second reading speech had a figure of \$3 trillion. Did that figure come from the NCA? Do you know the origin of that figure?

Mr R. McDonald—I have no idea where the origin of that is. You often see different figures about different things and you wonder where they come from.

Senator McKIERNAN—So it is not an NCA figure.

Mr R. McDonald—No.

Senator MASON—I trust, Senator McKiernan, that it was not the same estimate given to the cost of the millennium bug.

Senator McKIERNAN—I do not know, but I am still trying to find out.

CHAIR—Mr McDonald and Mr Tebbet, as I said at the beginning of your evidence, thank you very much for assisting us by varying your time of appearance before the committee. We are very grateful for that. There may be some issues, which come out of evidence from further witnesses, and we may follow that up with the NCA by correspondence. The committee intends to hold further hearings on this bill and, depending how today's briefing and hearings proceed, we may seek further evidence from the NCA at those hearings. Thank you both for your assistance.

[12.15 p.m.]

ARGY, Mr Philip, Vice President, Australian Computer Society

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

Mr Argy—It depends which version you have. The best way to check is that the second-last line of paragraph 3 should say ‘accept the need for’ rather than ‘or’.

CHAIR—It says, ‘Accept the need for specific provisions’?

Mr Argy—If you have the word ‘for’, you have the correct version.

CHAIR—Thank you, and thank you also for altering the time of your appearance before the committee. We have had some difficulties with some of our witnesses who apparently have a lack of awareness of Canberra’s weather at this time of the year, which surprises me somewhat. That has necessitated the changing of our timetable, so we are very grateful for your assistance. I believe your submission arrived at our secretariat office this morning and we are grateful for that. Senators may have had an opportunity to read it briefly, but could you assist us with a short opening statement, at the conclusion of which I will ask my colleagues whether they have questions for you?

Mr Argy—Very briefly, the Australian Computer Society’s position on the bill is one of trying to achieve the right balance. Plainly, computer crime is one that is of concern worldwide. Plainly, investigative authorities are frequently feeling thwarted in their ability to investigate and pursue criminal conduct because of people’s, shall I say, superior technical savvy. The society well understands and indeed supports the objectives of the bill, and indeed, in general terms, endorses the whole thrust of the officer’s report in the model criminal code, on which the bill is more or less based.

The real issues of concern to the society in this balancing exercise are trying to identify specific language in the proposed legislation that we believe is unnecessarily fuzzy or where it goes further than we believe can be justified based on what we understand to be those areas where investigative authorities have genuinely been thwarted. Listening to the previous witnesses, I must say that I was rather fortified in the view that I have held on this issue. For the most part, I felt very much in agreement with the view that Senator Ludwig put to one of the earlier witnesses—that is, that people are unsure of their technical prowess and so they err on the side of seeking more embracing powers of gathering and collecting information in case they need it.

The problem, I suppose, we have with that approach is that for better or for worse we start off with the default position in our society that you do not have to disclose your information to the government or to the authorities and that if they want it they have to justify getting it. To do that in the conventional world, people go before a magistrate, they swear information of a kind which enables an intelligent judicial officer to form a view about whether they need what they say they need and, if they have been persuasive, they will get a search warrant. The search warrant ordinarily, conventionally, is confined so that it goes no further than is objectively necessary to trample on the rights that people would otherwise have not to disclose whatever it is.

We have a different approach under the cybercrime legislation, and that is really the crux of the society’s concerns. Firstly we have the problem that—I do not want to be unduly pejorative, but I will use an expression that really makes the point—more than 90 per cent of judicial officers do not know the difference between a megabyte and a mosquito bite. In

practical terms that means that, if somebody comes before a judicial officer and is attempting to obtain a search warrant where the material is hidden in some technological manner or where some technological means are needed to get to it, the very honest position is that the judicial officer does not have the faintest idea whether they need what they say they need and will tend to take it at face value.

In those circumstances, the society says that it is not good enough to just have the existing regime apply, that the law needs to be much more explicit in trying to match what it is the investigatory authorities say they need with what they need. The way to do that, for example, is to ensure that the power to get the search warrant is conditional on it affording no more access than is reasonably necessary to obtain what is needed. By putting it that way—although at first blush they may obtain the search warrant and they may indeed get information—at least the court is then in a position to determine if it can be demonstrated that the defendant went beyond what was necessary. A provision which says that the evidence thus obtained will not be admissible is at least a bit of protection, whereas at the moment the regime that this bill establishes, it seems to us, is a huge trawling net—that is, because somewhere in Sydney Harbour there is a sardine that might have some value to some investigation so you go and trawl Sydney Harbour and order anybody who knows something about Sydney Harbour to help you.

Our concern is that that is just too broad and insufficiently delimited to be safe, I suppose, and that is the focus of our concern. It is not a problem with the principle, the thrust or the objective of the legislation. As I said, we readily accept the need for cybercrime to be met with cyberdetection and cyberinvestigation. As we have said in the submission, I think it is more a matter of education and training of the investigatory agencies and officers. In some cases it may be that there needs to be some legislative power but for the most part we remain fairly sceptical that the powers of the kind asserted to be needed in this legislation are needed in that form.

We have given you some examples but perhaps to illustrate during the introduction I will take you to a specific example that we have referred to at the end of our submission. Let us look at the clause that is added by clause 12 in schedule 2. That essentially says that, if you find anybody with any knowledge of a computer system in respect of which there is believed to be some information held that is relevant to a suspected crime, that person can have an order made against them that they provide the investigating officer with whatever information is needed to allow them access to that computer.

For example, Senator McKiernan might know a little about the computer network in Parliament House. Being a person who, within the language of this clause, is a person with knowledge of the organisation's computer network—to the extent that Senator McKiernan might know that the computers are connected to a network by a cable that runs under his desk—would be within the definition of a person against whom an order could be made that Senator McKiernan provide whatever information is necessary to enable the investigating officer to obtain access to any computer on that network. Senator McKiernan might say, 'I haven't the faintest idea,' and I would imagine a court would say that that is probably a good excuse for not obeying the order. But the terms of the legislation actually make it an offence not to obey the order and do not even offer the possibility that you cannot obey the order for a lawful reason.

Conventionally in provisions of this sort, you say a person shall not without lawful excuse fail to supply the information. The lawful excuse might be, 'I don't know the information that you want', or, 'It's not mine to give. I'm minding it,' or something else. But this legislation

does not permit of that. It really is a concern about where the balancing lines have been drawn. And they appear to us to be a little excessive.

We have emphasised the other key problem at the foot of page 1 of our submission. We do not understand why there have been some reasonably radical departures from the form of the provision that was set out in the model code which was in the Officers' Report. I think the committee has this document because Senator McKiernan was referring to some of the commentary earlier. The commentary is very useful, but sometimes it is hard to match it with what is in this bill. We have given an example. The one we have highlighted is the proposed section 477.2—which the explanatory memorandum, I am sorry to say, asserts is based on section 4.2.5 of the model code. But when you compare the two there are quite strong differences. The provision in the proposed bill is significantly broader and more encompassing. That might be fine and there may be a very good reason for it, but the explanatory memorandum asserts that it is based on the model provision. It is based loosely on it, but why is it different from the model provision? There is no explanation.

The third area is partly one that we suspect has been put there for constitutional reasons but perhaps is a bit of a sleeper with unintended consequences: it is the use of the term 'a telecommunications service'. Most people would appreciate that the Commonwealth has constitutional power in relation to posts and telegraphs, et cetera, which the High Court has said covers virtually all forms of telecommunication. The bill has, essentially, applied these proposed provisions in two different areas. One is where the Commonwealth is involved—either a Commonwealth computer or a Commonwealth agency or something of that kind; that is an easy nexus. The other kind is where a telecommunications service is involved. The definition of 'telecommunications service' is vastly broader than, for example, would be regulated under the Telecommunications Act.

It would include the network running in your home. If you have two computers joined by a cable, the link between them is a telecommunications service within the definition in this bill. That means that every single activity performed on a computer other than an activity performed on the physical computer that you are sitting in front of—in other words, any data accessed other than on the C drive of the computer you are attached to—must be effected by means of a telecommunication service, as defined in this bill. Therefore this bill will cover the field of everything.

It may well do so unintentionally. There was mention at some stage that there was going to be a provision preventing it from covering the field, so that state laws could operate concurrently. Our view would be that, by having this broad definition of telecommunication service, the bill has inadvertently confined state laws to applying to what you do on the C drive of a PC or on a stand-alone personal assistant or some such thing.

Senator MASON—Are you questioning the law's constitutionality?

Mr Argy—No. I am saying it is covering the field of everything and effectively ousting the operation of any state law. You might end up with state agencies prosecuting people, who would have a very sound defence that they have been prosecuted under unconstitutional legislation because what they did was something that involved a computer other than the one they were attached to which is the subject of a Commonwealth law and not the state law. Unless there is a provision which says explicitly 'it is not intended to oust the concurrent operation of state law', I would have thought that there was going to be a serious problem very quickly.

CHAIR—I regard both your submission and your evidence this morning as extremely helpful to the committee at this stage of our deliberations. Whether intentionally or otherwise,

you have very cleverly answered the questions that I had scribbled in the margins of your submission. Your paragraph 17 refers to the proposed new section 3LA. You used as your point of reference the cable under Senator McKiernan's desk providing him with enough awareness to be included in the broad of this proposed clause. You have suggested including language such as 'without lawful excuse' as perhaps a way of addressing that problem. Is it also a question of proximity—the person concerned, Senator McKiernan, being proximate to the alleged offence, or the suspected offence—as well?

Mr Argy—Yes. There are two parts to it. That is why in our paragraph 18 we have suggested that 'relevant' be inserted. Before an order can be made that Senator McKiernan assists, the knowledge he has would have to be relevant to the knowledge needed to obtain the access. At the moment, that nexus is not a requirement.

CHAIR—There should be some reasonable requirement for the person who is being dealt with in that manner to be reasonably proximate to what is going on?

Mr Argy—Precisely. It is easy to illustrate. Can I refer the committee to the proposed new section. It is clause 12 in schedule 2, which inserts the new section 3LA:

The executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance to reasonable and necessary to allow the officer to do one or more of the following—

and then a number of things are specified. The magistrate can grant the order if the magistrate is satisfied that there are reasonable grounds for suspecting that evidential material is held in or accessible from the computer. For the moment we will just park 'accessible from', because obviously the minute it is on a network it is accessible from any computer anywhere on the network. Then:

the specified person—

that is, the person against whom the order can be made—

is:

(i) reasonably suspected of having committed the offence ...

That might be one basis which most people would say is fair enough. But the next two bases are somewhat less proximate. If you are:

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; ...

There is quite a radical difference in nature of the three bases on which the magistrate needs to be satisfied. One would imagine that the investigatory authorities would never bother to have to go and prove something against the person who is the suspect. It is easier to go to the owner of the computer or an employee. If it is a corporate network, you would just go to anybody in the company who knows anything, because the specified person only has to have knowledge of the computer or 'a computer network of which the computer forms a part'. It seems to us there is just no matching. It must at least say the specified person has 'relevant' knowledge—relevance being 'relevant to what it is that access needs to be obtained to'. I am probably not articulating it very well.

CHAIR—I understand what you are saying.

Mr Argy—There is just this mismatch. As I say, our concern is that the mismatch is compounded because the most likely scenario when you come to seek a search warrant is that you either have the blind leading the blind or you have somebody who is not blind leading someone who, in terms of computer savviness, probably is blind and will not have the ability

to discern a lack of confinement of the sought-for order by reason of what is deposed to in what is put before the officer authorising the warrant. That is our concern.

There are multiple ways of addressing it. One, for example, is to say that the warrant has to be accompanied by a certificate from some independent person to say that the technological means sought are indeed needed to obtain the access. That would seem to be unnecessarily impeding an investigation. Our fall-back position is to say that, if the power does not extend beyond what is necessary, if it succeeded, the way to deal with it is that the court be required to disallow the evidence so that, in a sense, there will be a sanction for having gone beyond the bounds of what you had to do. I feel a bit like I am raising issues without giving a particularly satisfactory solution but, in the time available, we have not dreamed up a very simple and elegant solution, I must confess.

CHAIR—Thank you. Senator McKiernan has some simple and elegant questions.

Senator McKIERNAN—Thank you. I endorse the remarks the Chair made about your submission and your presence here this afternoon. It has certainly helped me tremendously. I do have empathy with the quote that is contained in paragraph 14:

... “government by the clueless, over a place they’ve never been, using means they don’t possess” ...

I can certainly empathise with that, and it might provide a subtitle for our report!

CHAIR—That is self-incrimination, I think.

Senator McKIERNAN—I do not have a problem with admitting to that.

Mr Argy—It is a lower-case ‘g’, I hasten to add!

Senator McKIERNAN—Do you have a problem with there not being a definition in the legislation of what a computer is, and, secondly, what a computer network is?

Mr Argy—No, I do not, for the very reason that was advanced earlier, when you asked the same question. The thrust of what the Australian Computer Society believes is appropriate is that if a person is doing any kind of criminal activity and there is information relevant to the investigation of that activity somewhere—and it is not on paper, but is in some electronic form somewhere—we do not see any need to impede the ability to get to it as part of the investigation by overlaying a definition of ‘computer’, which very likely would quickly become obsolete anyway.

Our view would be that we do not really care whether you use the word ‘computer’ or you use the word ‘thing’, as indeed the bill does use in a couple of places. It does not seem to us to be particularly relevant. The thrust of it, and the focus that we would like to see, is that you could just have about three sections which say that it is a criminal offence to maliciously make use of a computer, for whatever you do with it, and then allow the court to determine the gravity of what was done. Similarly, you could then say that a person shall not, without lawful excuse, fail to assist an investigating officer in investigating such an offence. That may be a very silly approach, but that, in our view, is the only kind of approach that makes sense.

What we see here is an attempt to articulate various manifestations of that kind of conduct that people have come across. It goes through four or five stages, ranging from the technical officer in the field finding that their powers are not sufficient—for example, somebody has done something clever to thwart them by putting in a password or whatever and they cannot get to what they want and they do not find explicitly in the current legislation something that forces that person to give them the password. If it was somebody who refused to hand over the key to a locked cabinet which had evidence in it, there would be no problem. The magistrate would say, ‘I order you to give the key.’ They just do not seem to be able to get

their brains around the fact that a password is simply an electronic version of a key. We accept that you might want to tweak the legislation so that the password or whatever access mechanism is there is treated analogously to the key, so that you provide whatever assistance is necessary to afford the access. We do not have a problem with that.

Senator McKIERNAN—In that sense then, are you happy to leave it to the judiciary to make that definition? Do you not see any difficulties with the judiciary determining what a computer network is for the purposes of determining whether an offence is committed against this particular legislation?

Mr Argy—No, I do not, because at the end of the day the critical element that we see as important is that there is the criminal intent. That is why I say we do not care whether the word ‘computer’ is used or the generic word ‘technology’ is used, if you commit a crime by using technology in the most generic sense you can conceive, why should it cease to be a crime? We would not like to see the position impeded by trying to define a ‘computer’. Indeed, I see no reason to even use the word ‘computer’. It can be any technology. Certainly in the class of offences that are in here that the commentary on the model code calls ‘preparatory offences’, there is absolutely no need for computer to be defined because it simply is exactly that: you are using some technological means to prepare to commit something that is otherwise an offence under some other provision of the code. Our view is reasonably straight forward: at the moment, if you fiddle books and records to try to get money by deception or to defraud somebody or for some other fraudulent or forged means, it strikes us that it is irrelevant whether you do it with a pen and ink, whether you do it with a laser beam, whether you do it with anything in between or whether you do it with means not yet discovered. I see no reason why the general thrust of the law should not be ‘thou shalt not murder’ and who cares how, you just cannot do it. So we do not have a problem with that.

Senator McKIERNAN—I am not going to go down that road. Just a further question, you expressed concerns about the powers that are given in the bill—powers not only to the investigating officers but also to the magistrates. In the second reading speech, which was not very long, the Attorney-General did give some space to the powers and supported the increased powers by referencing a draft Council of Europe Convention on Cyber-crime. Do you have a problem with our going to Europe to get authority on these matters? Is there not something anywhere else in the world that would give a better reference to the power?

Mr Argy—In a world that is interconnected, people can commit offences anywhere from anywhere. I think it is a world where the more international cooperation there is in sharing experience with the kinds of things people can get up to, the more useful it is. We would be disappointed if Australia tried to reinvent the wheel. With our population, the odds are that it has probably happened somewhere else before it has happened here. Innovative as Australians are, the odds are that doing something weird and wonderful with technology has probably been done somewhere else before it has been done here. Therefore, if the investigatory authorities overseas have devised an approach which seems sensible, we do not have any difficulty. Indeed, it seems logical to us to draw on that experience and reflect it here. We would rather have something here that is more standardised with what authorities are doing elsewhere than dream up something of our own—we do not want to preclude our dreaming up something more innovative than has been done elsewhere, but I do not have any difficulty with seeing what the European Council has done or the US or anybody else.

Senator McKIERNAN—The point being though they have not done it because it is only a draft convention.

Mr Argy—I understand that but one would imagine it reflects their experiences. Presumably, the draft has drawn upon experience of investigative agencies over there and activities that they have seen. It may well be that the only reason it has not been enacted is that they are not as efficient as the Australian legislators are.

Senator McKIERNAN—Do you not think that legislation as serious as this giving those enormous extended powers—there is a need for this legislation as well; it is not as though there is a party political obligation—

Mr Argy—It is a question of balance, as I said.

Senator McKIERNAN—Don't you think we should be depending on more than a theoretical—and that is all it is—code of behaviour in Europe or in any other part of the world?

Mr Argy—No, I would have to say we do not share that view, with respect.

Senator McKIERNAN—Are there not other examples in other parts of the world that we could be more reliant on rather than on something that is just at this stage—

Mr Argy—If I can give you another example from a slightly different context. The United Nations international committee on trade law passed a model law on electronic commerce. Australia was one of the first jurisdictions in the world to adopt and adapt that legislation for electronic commerce. Even though the code had been adopted in New York, Australia was more agile in adopting that code—and for good reason in that Australia saw the potential of a competitive advantage in making Australia e-commerce friendly before some other countries had got their act together, so to speak. Similarly, in this context, it seems to me that if work has been done elsewhere in the world that we can sensibly draw on and looking at it objectively it appears to reflect experiences and activities that are either similar to those we have had here or one can foresee would soon arrive here, I have absolutely no difficulty with drawing on that. It seems to me a sensible course.

Senator McKIERNAN—Thank you.

Senator MASON—Mr Argy, on that matter, Senator McKiernan mentioned the draft Council of Europe Convention on Cyber-crime. Are you aware of any other attempts to combat this evil?

Mr Argy—As the Officers' Report mentions, they have drawn fairly extensively on the European one, on the UK computer misuse act and on the US proposed code as well. They have reasonably thoroughly, as it were, done their homework in reviewing what everybody else has done and, as I say, that is why we support in general terms the model code that they have put together. It is in some of the detail where we have a difficulty. We think the general thrust is right and that it does put Australia in the position of not doing something weird and wonderful out on a limb and that we will, by having done it that way, be reasonably consistent with an international approach. It works both ways because it means that, if somebody from outside Australia commits some crime inside Australia, there will be very little difficulty in invoking those international cooperative processes because—

Senator MASON—There is interconnectivity.

Mr Argy—Let us look at a recent example on extradition. One of the grounds of a country resisting extradition is that the offence is not known in the country from which you are seeking extradition. If you transfer that example here, the analogy is that if most countries are broadly implementing the same principles, when you come to seek extradition or evidence from those jurisdictions, they will say, 'Yes, we recognise this. We have the same thing.' It is

not a difficulty that you will experience, and it seems to us useful to have that degree of standardisation on the principles that are being implemented.

Senator MASON—Let us look briefly at the detail. You argue, and I suspect members of the committee would agree, that investigatory powers should be—to use your words—‘delimited where possible’ but do you think that is possible today in a world where electronic data is shared so promiscuously? I am wondering whether perhaps technology has moved ahead of traditional concepts of criminal law, which has made it very difficult to delimit, for example, search warrants and perhaps the old days of the general warrant are coming back again under a different guise.

Mr Argy—I think that is exactly what is happening, and that is exactly our concern, with respect. In our view, whilst you need the balance, it is not appropriate to have a general warrant. You do need to force the investigatory agency to articulate what it wants and why with some degree of precision. You are quite right in terms of saying you might not necessarily know where the information is but you ought to be able to articulate at least the nature of the information you believe is held and at least the network or computer in which you believe it is held or from which it is accessible. There must be some threshold you need to meet to satisfy a magistrate or whoever that people’s rights to resist you ought to be displaced. I do not accept that, just because it is all too hard, they should simply turn up and say, ‘Your Worship, we believe someone has committed a crime, can we go and search every computer connected to the network?’ So that means anybody who is telecommuting and working from home who commits a crime in their home then, because they happen to be dialled into a network, every computer on that network is amenable to search—it simply, with respect, is inappropriate to do it that way. It may mean that they follow a train of inquiry and they have to incrementally get extensions to the ambit of the warrant. As I say, we accept that there is a balancing between impeding the investigation and protecting people’s rights. But it is a balance that we should at least adopt the pretence of trying to achieve, with respect.

Senator MASON—That is the rub though, is it not? On the one hand we have traditional concerns—and quite rightly so—with privacy, human rights and specificity with respect to warrants. On the other hand, we have new technological developments that seemingly make many of those traditional concepts redundant. I am not sure of the degree to which we will have to give up some of those traditional protections for the purpose of effective enforcement, particularly given, as Senator McKiernan said, if this is worth \$3 trillion a year in terms of the cost to the world community. I raise it because it seems to be the rub and I am not sure there is going to be any easy answer.

Mr Argy—I think that is right. Senator McKiernan probably was a little incredulous about the number—all of us are. It is very hard to quantify the value of computer crime, particularly when so much of it goes unreported because people are embarrassed that their security has been breached. If I can pick another example to try to address what you raised. There is a concept in the bill of ‘restricted data’ and the notion is that if you without authority access restricted data that is a more heinous offence than just accessing any other data without authority. The difficulty is that the way ‘restricted data’ is defined, it is anything that is basically not freely and publicly available on the Internet. I do not know of anything else, which is not kept at least under ID and password access, which satisfies restricted access.

Short of something that is available at a public kiosk or on the Internet without any access control, most people’s computers have some rudimentary access control which immediately converts it to restricted data and a significantly more serious form of crime. Again, it might be that the way to deal with it is to say to the courts, ‘We have done a general provision and

really at the end of the day it is for the courts in the sentencing process to focus more heavily on where the gravity of the conduct fits in the scheme of things and determine an appropriate penalty,' rather than try to articulate, which is the approach that has been adopted up until now, a cascading severity of crimes. Part of the problem is that people have tried to create a section that describes every experience that one has come across instead of trying to genericise it. That is why I say our preferred approach is to basically say if you use technological means to commit any currently known crime, then that is itself a crime—I do not have a problem with that—and indeed that is all they are really saying.

Senator MASON—Yes.

Mr Argy—One might well say, 'If it is already a crime then why do you make it a second crime just because you have used technology to commit the first crime?' But put that bit aside—

Senator MASON—I do not want to get into a debate with you, Mr Argy.

CHAIR—We do not have time for that, as it happens, Senator Mason.

Mr Argy—But the new offences in many ways are almost random descriptions of experiences such as hacking and unauthorised access today that people happened to have come across in recent years, and we have said, 'Let's make an offence for them.' But we see no reason why you should try to confine it to that, because tomorrow someone will dream up something different that is not covered.

Senator MASON—Law just reflects human experience, and I think we are at the threshold of a new one. So that is the problem.

Mr Argy—It does. In trying to summarise, we are concerned that there is not much greater focus on more explicitly requiring malevolent intent in the activity that is proscribed, because that is the one protection that people will have from the breadth of these provisions. If we could have that, we would be much more comfortable with what is otherwise very broad.

Senator LUDWIG—I was looking at your section 109 of your covering the field test. As I understand it, is this what you are saying that 476.4 is a saving provision which reads:

(1) This Part is not intended to exclude or limit the operation of any other law of the Commonwealth, a State or a Territory.

So at first glance it appears to contain a saving provision, which would mean that a state could still have a law which could work. But if you look at the definition of a 'telecommunications service' under the proposed Cybercrime Bill—I will never get used to that term—it states:

Telecommunications service means a service for carrying communications by means of guided or unguided electromagnetic energy or both.

So it broadens out from what we would regard as telegraphic communication; that is, what we would traditionally call Commonwealth telecommunications, such as lines and services—

Mr Argy—The kind of thing that could be regulated under the Telecommunications Act.

Senator LUDWIG—Yes. By defining it as 'telecommunications' service' effectively any Internet connection would be unguided electromagnetic energy, I suspect, between two computers. When you look at pages 6 and 7 of the EM under 'Proposed section 476.4—Saving of other laws', it says that it saves and a seamless—as they do—saving, 'ensuring there are no gaps in jurisdiction and also allows the computer crimes to be prosecuted in whatever forum is most convenient'. It then states what it thinks is the obvious and that the confidence maybe misplaced. It says:

As computer crime on internal computer networks does not involve use of the telecommunications system the Commonwealth cannot regulate this conduct.

That might be their view but it may not necessarily be the view that their bill seems to suggest.

Mr Argy—I think that sentence is simply wrong. It is plainly wrong given the definition of ‘telecommunications service’ is not the telecommunications system; it is broader than that. Although, interestingly enough, 476.4 is seeking to achieve what we were talking about. The issue was not so much with the division which contains 476.4. It is the words ‘this part’ in 476.4(1) which means only this part of the federal Criminal Code. But this Cybercrime Bill goes beyond that and inserts, as it were, analogous provisions in the Customs Act and in other pieces of legislation without the same proviso. For example, where equivalent provisions are inserted in the Customs Act, there is no provision inserted in the Customs Act that says—let me try to find it; they are provisions inserted by clauses 14 in schedule 2 and onwards. You do not find an equivalent provision saving state laws, so that if the conduct could be effected with the telecommunications service when the same definition, for example, were inserted in the Customs Act, you do not get the same saving.

Senator LUDWIG—No. That has been helpful. Thanks very much.

CHAIR—Thank you for assisting the committee with our deliberations today. It was very enlightening and useful evidence from the Australian Computer Society.

Mr Argy—Thank you for the invitation. If any further questions crop up, we would be happy to try and deal with them.

CHAIR—I was just going to say that. There may be some issues which arise during the course of this hearing and we will be having another hearing, probably in Canberra. So we may come back to the society by way of correspondence to clarify any of those points that are raised.

Mr Argy—We would be happy to assist if we can.

Proceedings suspended from 1.01 p.m. to 1.46 p.m.

CHAIR—The committee is going to take in camera evidence for a brief period from the Australian Federal Police. That means I will have to ask other witnesses who are in the room to leave for that period and then we will invite you back in.

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

ATKINS, Mr Michael Francis Charles, Special Adviser Law Reform, Australian Federal Police

BOXALL, Mr Jonathan James, Acting Team Leader, NII Incidence Analysis and Response Team, Australian Federal Police

WALTERS, Mr Mark Adrian, Acting Director, Investigations and Technical Operations, Australian Federal Police

CHAIR—Welcome. Mr Atkins, I now invite you to make an opening statement. At the conclusion of that statement, members of the committee will direct questions to you. I note, of course, that you will not be asked to give your views on matters of policy or reasons for policy decisions. If necessary, we will give you an opportunity to refer any such matters to your appropriate minister.

Mr Atkins—I have a brief opening statement. I will say a few words and then I will ask Mark to say a few words. The Australian Federal Police sees the emergence and increasing social governmental and economic reliance on information and communications technology as one of the major influences on the law enforcement operating environment both domestically and internationally. We would expect that this would continue for the foreseeable future. There is a very simple reason for this: ICT offers to criminals the same advantages as it offers to business, government and people generally—that is, you can conduct your affairs at speed and volume over long distance with a high degree of privacy and at a comparatively low cost.

It is important that we note that technology offers law enforcement exactly the same advantages but that it also increases the complexity of what we are about in that we need to harness those advantages as much as anyone else if we are going to be effective. We intend to provide the committee with some background on the AFP's role in relation to this technology to give you some idea of the operational issues we encounter and how the proposed legislation will support the performance of our functions under the Australian Federal Police Act and the use of our resources to perform those functions.

I think I should say at the outset that we appreciate the very clear need to ensure that law enforcement interests are considered together with other important values and in particular in this context, privacy. In fact, it is fairly clear that the amount of information that people put in about themselves when using this technology, either deliberately or disclosed in the course of using it, vastly increases the risk of unwarranted intrusion into people's affairs. Every fraudulent use of a credit card and every time someone goes through another person's system is an intrusion.

We see ourselves as operating in a highly accountable environment, and we have said this many times before. We have general public sector, the Commonwealth public sector, accountabilities. We have our own disciplinary regime wherein people can be required to answer questions. We also have a detailed and fairly strong complaints regime which is oversighted by the Commonwealth ombudsman's office. We see the performance of our functions as very much within that context of oversight as well as within the normal oversight of the courts in the course of criminal prosecutions.

While we see the impact of the technology as profound, we think it is important that it be seen in context and that we do not overreact. It is a new medium and it does provide opportunities to commit crime, but they tend to be traditional crimes. Crime is crime and the medium is, of course, highly relevant but it does not change its character. We can see it used in every aspect of what we do. In ACT policing we see it in street level crime, and we see it in

drug trafficking, fraud, money laundering and so on. More or less like ASIC increasingly sees it in market manipulation attempts and other corporate issues. So we see it as a form that is distributed across the whole range of our activity. We have one particular focus which is a bit different, and that is the use of the technology to affect national interests—what we call national information infrastructure protection, or NII. Unlike the implications of the technology across all of our activities, we have a concentrated capacity to deal with that in Canberra, and Mark Walters will talk somewhat about that.

The AFP has been involved in this area, both in an operational sense and in a policy sense, for some time. Because of the environments emerging, we are actively participating in the development by the Commonwealth of a consistent national approach to the issue. A very important element of that is cooperation with the private sector and attempting to assist the private sector to look after itself. It is partly altruistic because the more they look after themselves the less likely it is that they will become targets and, therefore, there is less flow-on work for law enforcement. All the other police commissioners have also recognised this. Mark will talk probably more clearly about this than I, but the commissioners have established an e-crime strategy.

CHAIR—Is that what was launched yesterday?

Mr Atkins—No, I understand that was something else. This was launched at the beginning of the year. I think the ABCI launch yesterday is an element of that strategy.

CHAIR—Oh, yes it was the ABCI.

Mr Atkins—Probably one of the more important observations we can make is that there is a lot of activity in the public sector on this. The big challenge is bringing it together, coordinating it and getting some consistency and common purpose while at the same time still doing the job of investigating it.

Briefly on the bill, we see the proposed legislation as an important step forward. There are a number of provisions in the bill that will assist us in our work and that make it clearer legally what we are dealing with when we are investigating the range of activities we look at. I do not think anyone sees this bill as the answer to everything. It is a first step. There is a lot more work that has to be done, but you have to start somewhere. We think it will not only make our life easier; we will be able to perform our job far more effectively with these provisions.

There is probably just one other point that I should have mentioned slightly earlier. The protection of the national interest is important—and Philip Argy touched on this—in terms of confidence in the Australian economy. Because it is such an important tool economically and socially, if your system is not secure and if people do not trust you, they are not going to use you. We see part of our role as assisting in underpinning confidence in this aspect of the economy and in the economy generally. We think it is probably a protective role which is of increasing importance.

CHAIR—Thank you. Mr Walters, I invite you to add anything that you would wish to. Doing so relatively briefly would probably be productive because that would give my colleagues some time to ask you some questions.

Mr Walters—Certainly, Chair. As my colleague Mr Atkins has highlighted to the committee, the impact of information and communications technology is quite significant on law enforcement in today's environment. This environment has created a variety of new challenges for law enforcement and via a number of fora and strategies the AFP is aligning itself to this environment to meet these challenges. I would like to address the committee this

afternoon on the AFP's capacity to meet these challenges, including our contribution to the many e-security and e-crime fora.

In pursuing its goals the AFP works in partnership with the police services of the states and territories, the National Crime Authority and other government agencies. The AFP has also established extensive international links through its international liaison officer network as well as the Interpol National Central Bureau and specific e-crime response mechanisms. The AFP is an active contributor in many fora progressing e-security and e-crime issues.

Commissioner Kelty is a member of the Australasian Police Commissioners Conference E-crime Steering Committee, which was established in March last year, and the AFP is a member of the working party chaired by the Australian Centre for Policing Research which is progressing a range of issues on behalf of the steering committee. Central to the objectives of the steering committee is the Australian e-crime strategy, which has been developed to provide a safer and more secure community by preventing and reducing electronic crime. The strategy has identified five focus areas: prevention, partnerships, education and capability, resources and capacity, regulation and legislation. The working party has prepared a work plan to support the implementation of the strategy, and the AFP is contributing to the progression of the five focus areas which are addressed in the strategy work plan.

The AFP also chairs the electronic crime law reform working party, which was established by the Australasian Police Commissioners Conference in March of this year. The AFP is also a member of the Action Group into the Law Enforcement Implications of Electronic Commerce, more commonly referred to as AGECE. AGECE was established in 1997 as a response to HOCOLEA's need to research the impact of electronic commerce on law enforcement and revenue agencies' ability to provide a safe community. AGECE has produced a number of issues papers addressing specific issues relevant to e-commerce and law enforcement and has established several subgroups on legal matters and cybercrime. The AFP is also a member of these subgroups.

The AFP is also involved in the Commonwealth's e-security national agenda, which is focused on the strategic objective of creating a trusted and secure electronic operating environment. The AFP is currently represented on the E-Security Coordination Group, the Critical Infrastructure Protection Group and a subgroup of that one, which is the critical elements working group. In addition, the AFP has also entered into arrangements with other Commonwealth agencies for the purpose of supporting national and international threat and vulnerability assessments, analysis and response. Recently there was a meeting held between the agencies involved in the national e-security agenda and the police commissioners' e-crime steering committee to bring together those groups involved in the e-security/e-crime framework to discuss a range of issues to make sure that they were avoiding duplication and to share ideas. It was resolved at that meeting that such a meeting should continue as an excellent forum or means by which we can progress these issues.

A number of recent studies revealed that there is a very low level of reporting of electronic crime. We understand that broadly this may be due to reluctance on businesses' behalf to admit vulnerabilities as well as a belief that law enforcement may not have the capacity to deal with these issues. Even with these relatively low levels of incident reporting, the AFP has been experiencing marked increases in referrals that we can categorise as electronic crime as well as the requirement for our electronic forensic support capability for investigations. The AFP receives referrals from a range of sources, including international law enforcement agencies, Australian government departments, other organisations, companies and individuals. Matters that are referred to the AFP are not always necessarily investigated. The

AFP assesses all matters referred to it according to its case categorisation and prioritisation model.

A number of recent studies reveal that there is a very low level of reporting of electronic crime. We understand that broadly this may be due to reluctance on businesses' behalf to admit vulnerabilities as well as a belief that law enforcement may not have the capacity to deal with these issues. Even with these relatively low levels of incident reporting, the AFP has been experiencing marked increases in referrals that we can categorise as electronic crime as well as requirements for our electronic forensic support capability for investigations. The AFP receives referrals from a range of sources, including international law enforcement agencies, Australian government departments, other organisations, companies and individuals. Matters that are referred to the AFP are not always necessarily investigated. The AFP assesses all matters referred to it according to its case categorisation and prioritisation model.

This model incorporates a number of criteria and only those matters which meet the relevant criteria are accepted for investigation. This process is quite important to the AFP's operations, because it allows us to deploy our resources to those matters which we believe have the highest priority. Unlike some jurisdictions, the AFP does not have a specialist computer crime team to investigate computer crime matters. Pursuant to our national teams models, those matters which are accepted for investigation are referred to investigation teams. However, we do have our electronic evidence teams, which provide electronic forensic support to these investigations. I will describe very briefly the role of those teams shortly.

We have, in the past 12 or 18 months, established an NII Incident Analysis and Response position in our National Operations Monitoring Centre. That is the role which Mr Boxall performs. In addition to responding to critical NII issues or incidents, the role is also responsible for analysis of non-critical incidents, to identify any related activity which may constitute a critical NII issue, as well as the identification of strategic issues and trends. The role also provides advice to AFP management on NII issues. Another important role of that is providing what we might loosely call first aid, where a matter might be referred to the AFP. It might not be accepted for investigation, but through that role we can provide first aid or advice that may, if the incident is live, assist in dealing with or responding to that incident.

I mentioned briefly that we have an electronic forensic capacity. Whilst AFP officers are becoming more comfortable and more familiar with the electronic environment and its impact on criminal investigations, it is probably fair to say that the vast majority do not have the technical skills to be able to search for evidence on electronic systems. To cover that gap, we have a number of electronic evidence teams, which are located in Sydney, Melbourne, Brisbane, Perth and Canberra. The role of these teams is to recover evidence from electronic systems. As mentioned previously, these teams do not actually investigate matters; however, they are increasingly supporting our investigations, not only for the AFP but for a number of other agencies, including the National Crime Authority and state police services, as well as other Commonwealth agencies.

As a final point, the AFP also recognises the increasing need for professional development in this area. As the development and use of information and communications technology increases, so too do the demands on the AFP to train our people. It is fortunate that this week the AFP has launched its inaugural e-crime training program. The program is designed to upskill the organisation in terms of the electronic environment and, in keeping with the theme of the subject matter, the majority of the program is being delivered online. This not only delivers efficiencies for the AFP in terms of its training delivery, but it also ensures reinforcement of that subject matter, because people are doing the program online.

I understand that we are working with the NCA in relation to this matter. The program also includes a practical component, which will develop investigative skills to search electronic systems and seize evidence where appropriate. We are also now commencing the development of a second-tier training program, which is designed to provide investigators with enhanced forensic skills to search and seize electronic evidence. That is all I would like to brief the committee on in terms of what the AFP's capacity is in this particular environment.

CHAIR—Thank you. I will just take up the point you made at the end there in relation to the e-crime training program delivered online. Who are the participants in the training program? Are they agents who are already involved in computer crime, broadly speaking, or is it anybody who has an interest and wishes to upskill?

Mr Walters—The program is open to everyone in the AFP. We are hoping to have as many members of the AFP as possible, if not all members, trained through this program, because it is not only addressing what some people refer to as hacking, or other intrusive crimes, it is introducing people to the broader electronic environment, and just about everybody in the AFP, regardless of their job, is impacted on by that environment, so it is a very broad education program. But we are trying to have our investigators who are dealing with these matters prioritised in terms of the training on that program.

The feedback already in the first four days from some of the participants on the program is very positive. They are providing feedback on the program which will obviously be considered and used to enhance the program as we go. It is a very dynamic environment, and we constantly monitoring that to make sure that the program is updated to reflect that environment.

CHAIR—In terms of the hows and whys of that, was everyone invited to participate by email? Do you know how that was done?

Mr Walters—Yes, there was a general advertisement for applicants to apply for that program. From memory—and I can confirm this by some inquiries—there were 25 participants in each program, and there are four programs scheduled for this financial year.

CHAIR—It could take a while to train everyone then.

Mr Walters—We are hoping to increase that capacity as the program develops. The online training component is about six weeks, and that is followed by a two-day practical hands-on session.

CHAIR—Thank you for that information. That is very helpful.

Senator McKIERNAN—We are all on a big learning curve in regard to this bill and are finding out more and more as each set of witnesses appears before us. Thank you for reading out the pluses. Earlier today I described to one set of witnesses that this was a dramatic increase in the powers of law enforcement agencies in Australia. Would you agree that that is the case, that the bill gives those increased powers?

Mr Atkins—There certainly is an increase in power. I do not know if it is dramatic. I am looking at it from what in fact we are seeing and what in fact is needed to be able to operate effectively in the environment. It certainly is an expansion. There is no question about that. You have got the fundamental question of: here is a new type of creature—'a new operating environment' is the words I use—and how do you operate in it effectively? It gives us an accountable and firm basis for doing the work that needs to be done, and that is why I do not see it as dramatic. I think it is accountable. I see it as an extrapolation of the mechanisms we had in the paper world.

Senator McKIERNAN—Let us take the search powers. When you apply for a search power—this morning I used the analogy of a filing cabinet; in this case it is a computer—because the computer is networked it is actually much more than just a search warrant on a filing cabinet or a computer; it can be a search warrant on multiple computers. Is that not dramatic compared to where we are at the moment?

Mr Atkins—As I said, I see it as an expansion. But I think the analogy of the filing cabinet—it is funny how we keep using analogies in this area, but I suppose we have to—is to some extent correct or is valid. It falls down in some regards in that you need to be able to get into the filing cabinet, and what happens when you get in there and it is all in code? What do you take, what do you not take, if it is all in code? How do you work out what you want to take? You are going to end up trying—if you know it is in code—to take the whole cabinet to have a look at it. The protections stem from the fact that you need to get the warrant. The terms of the warrant are going to control what you do, the extent to which you can control—the sardine analogy was used this morning—

Senator McKIERNAN—A bit fishy.

Mr Atkins—The fishing trip—fishing for a sardine. My colleague from Attorney-General's can possibly better answer the question than I can but, as I said, it certainly is a significant expansion. I do not see it as dramatic, but your point is there.

Senator McKIERNAN—I got an understanding that, from your point of view, the search warrant, when issued, will be issued as broad as possible to assist you—and the AFP, NCA and other law enforcement bodies—with the investigations. You will want it as broad as possible. So you are targeting one suspect, that suspect's technology is networked to other technologies around the place and your search warrant will allow you to get into those bits of equipment or things, will it not, even to the extent of copying without their knowledge? Perhaps Senator Ludwig—we are using analogies again—is suspected of some offence and you get a warrant to examine his computer equipment and because his computer equipment is logged into the parliamentary network, as in turn mine is, you can actually get into mine as well, and you can look at mine and copy mine without necessarily telling me.

Mr Atkins—As long as the original conditions of the warrant apply. In other words, it is restricted. It is not just a fishing trip; you have to have grounds for looking for the evidence as you go on and on.

Senator McKIERNAN—We are both members of the Labor Party. That is why I did not—

CHAIR—That is a good start for reasonable grounds, Mr Atkins. I would be going right down that road.

Senator McKIERNAN—The point I am making is that that could be done—I am trying to bring it down to a personal thing, so that I can understand it, rather than anything else—on the basis of a warrant without my knowledge, and you could copy everything that is on my laptop, provided I have opened it, without my knowledge. Surely, that is a more than significant expansion of your powers.

Mr Atkins—I will go back to my original point that there is clearly an expansion of powers. Trying to characterise it as dramatic or significant probably is moot. It is appropriate to the environment we are trying to operate in, the significant complexity. There are probably two observations. Firstly, with all of this technology people pretend they are not dealing with people, but the fact is that the transactions that Jonathan has talked about that we see are created or caused by people but the actual manifestation is automatic, and it is getting beyond

that, lifting that veil from the machine to the person, that is one of the perplexing factors in this new environment which I do not think anyone has properly come to grips with yet. That partly explains that point. You are following this almost electromagnetic trail to find a person. Sometimes when you walk in with a warrant and you seize a machine or you are interrogating you have a person, but you might not have a person. You may simply know this machine has been involved in this transaction. As Mr Boxall explained, you can have a series of transactions on machines that are involved in something that is quite remote from the actual person who is causing it.

CHAIR—What privacy protections are in place to protect material of other persons who are remote, as you describe it, which is totally unconnected to the suspected offence and may be collected in this process?

Mr Atkins—Can I ask Geoff McDonald from A-G's to answer in terms of the operation of the provision?

CHAIR—Not right now you cannot, no; but later you can.

Mr Atkins—Okay. The AFP have in place rules as to how you can use the evidence. Of course, it has to be of evidentiary value and the usual search warrant stuff applies. Second, we are bound by the Privacy Act and the information privacy principles apply to us, and we all get audited from time to time.

CHAIR—Audited by the Privacy Commissioner?

Mr Atkins—Yes. We also have—and I can get these provided to the committee—quite strong internal instructions and guidelines as to the use of this material.

CHAIR—We would be very pleased to see those.

Senator McKIERNAN—The further expansion of the powers is that the officer who is executing the search warrant can apply to a magistrate for an assistance order, under which that individual would have to assist. We had a great analogy about how that would operate in the cables on my desk in my parliamentary offices. This is an expansion of the powers. Those powers are not currently contained in the existing Criminal Code.

Mr Atkins—That is right.

Senator McKIERNAN—The Attorney-General, in the second reading speech, drew the authority for those powers from the draft Council of Europe Convention on Cyber-crime. That is a draft convention and, as I understand it, it is in its 25th draft. It is not necessarily an authority, is it? Do you know of any country in the world where there is a law in existence in regard to this, rather than a convention which is in draft form?

Mr Atkins—We can take that on notice again. A-G's might be able to answer it.

Senator McKIERNAN—We will follow it up with A-G's. The final question from me is: we understand—although we have not seen your submission yet—that the AFP is strongly supportive of this legislation. Are there any downsides in the legislation for you? Are there any areas which the AFP consider to be possibly problematical, as opposed to—

CHAIR—Isn't their answer usually that it does not go far enough?

Mr Atkins—It is an odd area. A lot of legislation is possibly problematical—particularly in an environment like this, which is very new and people are coming to grips with it with a very low experience base—simply because you cannot, by its very nature, really know what is going happen, which is the point I made earlier. We think it is an area of policy, of law, of law enforcement practice and of business practice, which is going to have to constantly be

revisited as experience grows. It is a fascinating area, but it really is full of uncertainties at the moment. I cannot anticipate, from an AFP operational point of view, any major difficulties for us through this legislation. Having said that, as we all know, some wonderful models of legislation have been passed by various parliaments in the past and you get bitten by the unexpected. But there certainly is not anything here that currently worries us.

Senator LUDWIG—Some of these questions may have been addressed in part, but how many complaints have you received in the area? Are you able to say, in terms of what you would identify as cybercrime, or as e-commerce?

Mr Walters—I can answer that. These figures are based on the year 2000-01, from 1 July 2000 to 30 May 2001. During that time, the AFP received 320 electronic crime referrals, and those were e-crime referrals based on the categorisation within our promise, which is our information management system. Approximately 54 per cent of the e-crime referrals to the AFP related to child pornography and paedophilia activity on the Internet and, of these referrals, three-quarters were from the Australian Broadcasting Authority regarding potentially prohibited Internet content based outside Australia. The next most common type of e-crime referral to the AFP involved intrusions or unauthorised access to computer systems, colloquially referred to as hacking, which represented 16 per cent of our total referrals. Denial of service attacks and referrals relating to Internet viruses, trojans and worms accounted for eight per cent of referrals. Other types of e-crime referred to the AFP include threats, harassment and stalking over the Internet, which were eight per cent, and fraud six per cent. All other referrals, such as intellectual property, piracy, counterfeit offences and the sale of illegal items via the Internet together accounted for less than 10 per cent of total e-crime matters referred to the AFP.

Senator LUDWIG—Without the Cybercrime Bill, to your knowledge how many of that total would currently not be able to be investigated and, potentially, prosecuted?

Mr Walters—I am probably not in a position to provide a very accurate answer for you on that question. However, I can take that on notice.

Senator LUDWIG—Yes, please. You say there is a number of complaints. The particular statistic I was looking for was: of the number that would get through the hoop of your case categorisation and prioritisation model, how many could not be dealt with today because you lack either the investigative methods or because there is no law that is being offended? You would envisage joint operations with Customs or state police services in some of these areas, I suspect. How many of that number would require the Cybercrime Bill to enable you to do that? How would it be proceeded with? If either Customs or the state police services do not currently have the powers given under the Cybercrime Bill, how do you go about investigating those should you have the Cybercrime Bill? I take it that you want to take that on notice.

Mr Walters—Yes.

Mr Atkins—Yes. We will attempt to deal with that in the submission.

CHAIR—Thank you, that would be helpful.

Senator LUDWIG—Given the range of matters that you have mentioned including trojans, worms, threats, countermeasures and everything else, is the Cybercrime Bill sufficient to cover all of those issues that you have raised or that you are aware of? Mr Boxall, you particularly would be aware of the range of current types of operations that hackers and the like might undertake. Is the Cybercrime Bill comprehensive enough to deal with all of those current issues that you are aware of or envisage?

Mr Boxall—In terms of the issues that I deal with, I would say yes. I would not say that the offences are making a huge leap from what we currently have. The main change that would impact on me would be provisions relating to unauthorised access. I have had discussions with Michael Atkins on that, and we do not think it will have any real impact on what we are doing now.

Mr Atkins—The clarification particularly of the communications events, the spamming type offences, is of value.

Mr Boxall—The main benefit, as I mentioned previously, will be the effect on the impairment of communications. I see that as a real step forward.

Senator LUDWIG—You mentioned that you saw this as the first step—an extension of the current law into cybercrime—and you might envisage a time where there is a second step taken, or a further step taken. What do you mean by that? Is this only the beginning of a raft of legislation that might come before us?

Mr Atkins—I was thinking more in terms of an ongoing assessment process, a testing process. It still is comparatively early days with the technology. The AFP thinks it is inevitable that, as our experience in this area develops and as the technology develops, better ways of dealing with things may become apparent; there may be flaws in the way in which we operate which may make it easier to use law; or alternatively defects in the law may appear. I am certainly not saying that we think there will be legislation every year. But this is the first coherent step in developing what I call the policy and legislative infrastructure, which is going to not only support law enforcement operating in this environment but also provide support to the private sector operating in this environment as well. I was trying to get to that concept of underpinning confidence, of moving away from the various analogies which are used in relation to information and communications technology.

Senator LUDWIG—How will you ensure that search warrants issued in the cybercrime area are in truth not general warrants? What is your mechanism? It would be so much easier just to do a general warrant—and I hope you don't agree with me!

Mr Atkins—No.

Mr Walters—I think we would be applying the same provisions and guidelines as we do for search warrants presently. They are very prescriptive as to the way in which we seek and are issued search warrants. It is incumbent upon us to ensure that we adopt those guidelines.

Mr Atkins—We see ourselves as very much operating within a framework of accountabilities. Apart from that, there is also highly pragmatic discipline: administrative litigation surrounding search warrants is incredibly expensive and time consuming. You will lose evidence; that is the ultimate discipline. If your warrant is too wide or if your warrant is inappropriate and gets knocked out, you will lose your evidence. I know from my previous history in the AFP, when I was responsible for defending a number of challenges to warrants in various guises, that it is very time consuming, extremely expensive, and you inevitably do not get anywhere near a prosecution for years. So there is a very pragmatic discipline to get it as right as possible.

Senator LUDWIG—Have you exercised any warrants in this area for computer searches, or something similar? If you have, could you make one of these available to give us an idea of what you do—with all the relevant names and people removed?

Mr Atkins—We will look into it and we will do it.

CHAIR—So you will take it on notice?

Mr Atkins—Yes.

CHAIR—I was thinking, Mr Boxall, that perhaps I should take my colleagues on a popular education cultural excursion to see *Swordfish* as a crash course in worms and associated matters. Senator McKiernan would enjoy it enormously.

Mr Atkins and gentlemen, thank you very much for assisting the committee this afternoon and for your evidence. You have taken a number of matters on notice and we would appreciate advice on those as soon as possible. There may be other issues raised during the rest of this afternoon's hearing, on which we may come back to the Australian Federal Police.

[3.00 p.m.]

CHIDGEY, Ms Sarah Jane, Legal Officer, Criminal Law Branch, Attorney-General's Department

McDONALD, Mr Geoffrey Angus, Assistant Secretary, Criminal Law Branch, Attorney-General's Department

ORLOWSKI, Mr Stephen Robert, Consultant, Attorney-General's Department

CHAIR—I welcome witnesses from the Commonwealth Attorney-General's Department. The Attorney-General's Department has stated that it will not be making a formal submission to the committee and is here today to provide the committee with a public briefing on the Cybercrime Bill 2001—for which the committee is grateful. I do think, though, I need to note that, as you are acutely aware, the Attorney-General's Department is appearing much later in today's proceedings than planned. Other witnesses have rearranged their schedules to assist the committee with the proceedings of this hearing, and the committee has rearranged its work plan today to accommodate the lateness of the department in arriving. I would like to say that you fell victim to the vagaries of the Canberra winter fogs, but in fact in my view they are not vagaries; they are certainties. That is why our secretariat, Hansard and other Canberra based witnesses travelled in such a way as to avoid this problem. Not specifically in relation to the witnesses here, but in relation to the department itself, it has happened before. This is not the first time the committee has been inconvenienced in this way, and I would appreciate very much the department's assistance in trying to avoid it ever happening again.

Mr G. McDonald—I apologise for that. It was mainly due to my own inexperience at travelling down here, I guess. I apologise to the committee and to the other witnesses. I will take steps to make sure it does not happen again.

CHAIR—Thank you, Mr McDonald. I invite you to begin your briefing. At the conclusion of that, there will be members of the committee who certainly have questions for you. I note that you will not be asked your views on matters of policy or reasons for policy decisions and that, if necessary, we will give you the opportunity to refer those matters to the appropriate minister. We have had the opportunity to hear from the NCA, the AFP and the Australian Computer Society so far today, so we have come some short way in our understanding and appreciation of the bill. Mr McDonald, I am sure your usual very helpful submission will assist us in furthering that, and we will come back to questions at the conclusion of that.

Mr G. McDonald—The proposed computer offences and enhanced law enforcement powers reflect changes in technology and community use of computers since the existing provisions were enacted in 1989 for the offences and in 1994 for the existing search powers in relation to computers. While this bill is probably one of our slimmer volumes, it addresses important gaps in the existing law. The gaps are by no means minor. We have seen in recent years enormous damage as a result of malicious misuse of computers. Indeed, if similarly-minded people were to let themselves loose with a bulldozer in the Sydney central business district, I doubt they could cause more damage than the likes of some of those who have orchestrated some of these web-borne attacks, denial service attacks and the like—some of the more publicised ones anyway.

You will note that the Model Criminal Code report, which was released earlier this year, deals with computer offences as part of the chapter that also deals with damage offences. I think that is probably appropriate. These offences are really all about causing damage and,

like damage offences, the activities can range from something quite minor right up to having quite catastrophic consequences that could destroy a business, damage it or even cost jobs.

It is therefore appropriate to set the penalties and the method of dealing with this conduct on a similar footing to damage offences. If you have a look at these offences they are very similar to those in terms of the range of penalties and the harm-based approach. It is for those reasons that every attorney-general in this country has agreed to give priority to updating computer offences and governments have embarked on an effort to get not only modern and effective provisions but also some consistency around Australia. The need for consistency could never be more self-evident than in relation to this area. You will find that the recently enacted NSW computer offences are the same as those that are in this bill, and work has started on similar legislation in other states and territories. Hopefully, by this time next year Australia will have some of the most effective and modern laws in this area right around the country. That is our hope.

The level of cooperation between jurisdictions is evidenced by a copy of a letter from the New South Wales Acting Minister for Police, which I will table at the end of the process, where New South Wales raises a potential problem with one aspect of the bill which was not detected when we were developing the bill together with New South Wales and other states, and that is in relation to state search warrants. It would appear that we would need to put in a provision which ensures that those search warrant provisions are not adversely affected by the bill. If you read that letter you will see that there has been a very cooperative approach between the jurisdictions. Indeed, the attachment asks us to put their letter before your committee, which also indicates that. Whilst a general principle and activity justified by or under a Commonwealth law is excused under section 10.5 of the Criminal Code, the same is not the case where activities are authorised by state law, and that is why this needs to be addressed.

I should say that those who have reservations about the bill are quite often driven by misconceptions that the offences might apply to authorised activities. Some people have misunderstood that point. Of course, the offences are limited to where conduct is unauthorised. The improvements to the bill in relation to search powers build on provisions which were enacted for this purpose in 1994. We have circulated a paste-up copy of the bill, which I think I might have on a previous occasion promised to do in the future when we had some difficulties. If you look at that paste-up you will see that it indicates what the previous provision provided for and how this is different.

On the matter that you were speaking to Mr Atkins about earlier in the piece, if you actually compare particularly the issuing grounds between the old and the new you will see that in some respects those issuing grounds are clearer and more precise, therefore ensuring that these warrants are certainly not general warrants and the executing officer or constable assisting must believe on reasonable grounds that any data accessed by operating the electronic equipment might constitute evidential material and he or she may copy the data to a disc, tape or associated device brought to the premises or, if the occupied premises agrees in writing, copy the data to a disc, tape or other associated device at the premises. If you look at that document we have circulated you will see that this fits right within the very specific warrants regime that we already have. If the AFP or law enforcement step outside of the specific approval that has been given by the magistrate in relation to the warrant, then they will obviously have difficulties with the evidence.

Senator McKIERNAN—I am sorry to interrupt. You said you had circulated the paste-up. Was that in an encrypted form?

CHAIR—It has been sent to the secretariat. I am not sure that the secretariat has distributed it to us, but I now have a hard copy so we will work from that.

Mr G. McDonald—That will help a little in seeing that this is not all one-way traffic and that there is some harmonisation of what we are doing with computer offences and other aspects. There was some mention of whether this idea of getting someone to assist is particularly unique, and the answer to that is no. If you look at the explanatory memorandum, in item 12 we have mentioned some other examples of assisting provisions which are already in Commonwealth legislation going back 20 years, and I think we can help you with the international stuff too. I can tell you that in the United States there are quite amazing powers in this area, and it is correct to say that this is a fairly conservative package.

If you look at the draft cybercrime convention, you will see there are provisions in there which go far further than this convention. For example, there is the capacity to have remote searches, documentation retention requirements and quite a few requirements like that—and also in UK legislation, as my colleague has just mentioned. The impression that we have got in our discussions in the development of this bill is that the AFP see this, and certainly we see it, as legislation which has developed out of experience with the existing legislation.

I was involved with the development of the existing legislation in 1994, and when I look at it again it reminds me perhaps of my mortality. It was quite interesting looking at it again and comparing what we are doing here. We certainly saw computers at that time—in the sense of them being much larger mainframe type things, and even the personal computers—as fairly delicate things which could not be moved around very much. Certainly, a lot of the feeling at the time was that we do not really want stuff moved off the premises, because the police might break it or something like that. What has happened since then, even since 1994, is the incredible portability of computers and the ease with which material on them can be downloaded quickly and taken away. There are considerations like that and there are also other considerations—for example, the assist provision. In 1994 our feeling was that you do not really want anyone that might be involved in the matter anywhere near the computer because they might just press one of those little buttons and, then, goodbye all the evidence. However, the capacity now to just be able to copy everything quickly on zip disks and things like that and then to ask the person to assist in terms of identifying aspects of it have certainly changed the environment.

Mr Orlowski could probably tell us a little bit about the linking aspects of it. He is my hired computer expert. I am a bit scared that Senator Ludwig might ask me how email actually works, or something like that, and I might not be able to give a technical explanation that suffices. However, the capacity to be able to put important information through a link on a remote site is there. If, within the confines of the search power, police were not able to do that, then there would be great difficulty.

I will point out, though, that the old provision probably enabled the police to do that anyway. The legislation says that the executing officer or constable assisting may operate electronic equipment at premises to see whether evidential material is accessible if he or she believes, on reasonable grounds, that the operation of equipment can be carried out without damage to the equipment. With incredible foresight in 1994, the people that legislated this obviously were able to think of this access issue. But it is not nearly clear enough, and we have, as part of the Criminal Code project and in all of our efforts to codify the law in this area, made the law clearer. The clearer the law, the better it is, in terms of the police—and the community—knowing what they can and cannot do.

I should add that other areas that have changed since the period 1990-94 include the incredible interconnectability of computers and the mass use of computers which has grown exponentially in that time. Given the fact that we usually associate most crime with physical evidence of various types and here we are working in a world where there is very little physical evidence, it is but a modest enhancement of police capacity when seen in that context.

Finally, in preparing this bill we have been careful to watch international developments and, in particular, the draft cybercrime convention. There has been some mention of that, and I think it is up to the 27th draft. It is true that it remains a draft, but the target is to finalise that this year. We have merely picked up the less radical elements of that, and by 'less radical elements' I mean the offences that we have and the basic powers that we have here. The more radical elements deal with issues like remote access to computers and record retention requirements and so on. In the vicinity of 60 countries—a very large number of countries, and not just the countries in Europe—have been involved in developing the cybercrime convention. Whatever is agreed in the end, it will be the world standard. Our difficulty is that we have laws that just are not up to scratch and we need to do something now, so I commend this bill to you.

CHAIR—Thank you. Mr Orlowski, did you wish to add anything at this point?

Mr Orlowski—I would like to do something a little historical. Having been involved with both the 1988 provisions and the current one, I would like to give a quick overview of the computing environment at the two times, to give you an idea of why some of these things are changing.

CHAIR—If you can make it brief and historic that would be useful.

Mr Orlowski—In 1988 computers were typically mainframe with dumb terminals. There was a little dial-up access availability, which was using telephone lines to connect, and there was dedicated line connection. Nowadays the Internet has changed all that. Connectivity is a major issue and data storage is becoming diverse. One of the problems is that material may not even exist on a single computer but may be brought together from elements on different computers to make up a document at a particular point in time. That document, as it exists, does not exist on a single computer but pulls down elements from different computers. Another problem we have been facing lately is that there is a tendency in the hacking community to download data onto someone else's computer so that it cannot be found on the hacker's computer. That is a fairly common approach and one which needs to be addressed within the context of this bill.

Basically, what is happening is that there is this increased connectivity that, in itself, opens up the whole network to other people. There is an availability to just move data all over the place, and that is why we have had to look at some of the provisions we had in that original legislation—in particular, the impeding communications requirement in the original act. While it had some provisions in there that may or may not have been able to be used in the case of a denial of service attack, they were never really designed with that in mind. That is why we had to revisit the communications and the importance of those linkages, which is how the data is all worked together.

CHAIR—Thank you very much. We will move to questions. I just want to touch on one question with you, Mr McDonald. We have an interesting submission from the Australian Computer Society. As you know, submissions do not close until tomorrow so you may not have seen it and I understand if that is the case. The submission comments on the divergence from the recommendations, or the substance, of the Model Criminal Code and the

recommendations of the Officers' Report and makes some comments about where the bill moves away from those. Can you make any comment on that?

Mr G. McDonald—I find that surprising. The only areas of divergence in relation to the offences relate to the jurisdictional aspects of the legislation. Structurally, we made a couple of minor changes, but really I find that fairly surprising—unless the reference is to the fact that we have enhanced the law enforcement powers in it.

CHAIR—It particularly refers to definitions, to clarify that for you. I would be grateful if you would have a look at the Australian Computer Society's submission. Perhaps Mr Philip Argy's evidence from earlier today would also assist you in considering that point.

Mr G. McDonald—Yes.

CHAIR—The NCA were before us this morning. Their submission—also received today, so you probably have not seen it—makes reference to the Commonwealth Action Group into the Law Enforcement Implications of Electronic Commerce, which I understand to be chaired by AUSTRAC, and also to the E-Security Coordination Group and the Critical Infrastructure Protection Group. Is the department part of all three of those?

Mr G. McDonald—Yes.

CHAIR—What is the status of progress of the work of those three committees? Would you describe it as being some way down the road or a long way down the road?

Mr G. McDonald—No. Those groups overview a whole range of activities. With this bill, we were able to consult with various departments and agencies within the Commonwealth and elsewhere, and this bill is very much part of the process that is going on there. In relation to those groups, I was at a meeting just yesterday where—

CHAIR—Which of the groups?

Mr G. McDonald—Of the AGECE group. I have also been at meetings of the other group. They have quite a vast program of activities, some of which are before the government for decision. I also have here more details of the ABCI activities—including a nice folder.

CHAIR—Good; I was wondering about that. That was the announcement made yesterday by the West Australian Police Commissioner?

Mr G. McDonald—Yes, and that is obviously a cooperative effort between the various jurisdictions. The main thing in that, of course, is the idea of having an e-crime desk in terms of the ABCI pooling information and intelligence and enhancing cooperation between the various areas in the way that they do in relation to a lot of other issues. Again, I will table that.

CHAIR—Thank you, that would be helpful. Would you say that the operation of those three groups to which we have been referring gives the Commonwealth a reasonable overview of activity in this area at the moment?

Mr G. McDonald—Yes. Certainly the AGECE group is focused on looking at the law enforcement difficulties and trying to ensure that there is a carefully reasoned law enforcement position on the crime issues. The e-security group looks at a wider range of issues that involve the broader groups ranging from Defence to the communications department and so on. The representatives of the AGECE group, or the law enforcement group, attend the broader groups. AGECE ensures that there is ample discussion between the law enforcement people. If it did not exist, when they went along to the larger group it might be that some of the issues that concern them would get subsumed. These types of mechanisms are ones which are always under review. It might be that in another year or two we will have a

different mechanism, but the most important thing is that people are talking and understanding each other's perspective.

CHAIR—What does the Critical Infrastructure Protection Group do?

Mr G. McDonald—Unfortunately, I am not as well versed on the Critical Infrastructure Protection Group as I should be.

CHAIR—Do you know who chairs it?

Mr Orłowski—The Attorney-General's Department chairs it—Peter Ford.

CHAIR—Who chairs the E-Security Coordination Group?

Mr Orłowski—The National Office for the Information Economy.

CHAIR—And AUSTRAC chairs the AGECC?

Mr G. McDonald—Yes.

CHAIR—Do we need three?

Mr G. McDonald—I do not think I can give an opinion on that, mainly because I am the lawyer, I guess, and I have been brought in to do a specific job.

CHAIR—That is not a bad thing, Mr McDonald—many of us are.

Mr G. McDonald—Yes, that is right. I have brought in to do a specific job here. I think you have seen me masquerading as an expert on many different topics, and now it is cybercrime. The really great thing about those groups is that there is at least proper interaction between people, and people become aware of what is going on. I might add that I am not very good on names, so no doubt I will have a few people to apologise to when I get back.

CHAIR—Mr Orłowski, did you wish to add something?

Mr Orłowski—I was going to clarify that Australia also chairs OECD and APEC activities in this area—and has done for quite a few years now—so it is at the leading edge of the whole area of e-security and information security.

CHAIR—Thank you very much, that is useful information.

Senator LUDWIG—I have a couple of matters that were raised earlier today, but I thought if I draw your attention to them you might be able to deal with them either now or shortly or to take them on notice. One of the issues raised in an earlier submission by the Australian Computer Society related to the savings provision under proposed section 476.4.

The concern was twofold. If the saving provision was only under this part, did it only then relieve section 109 covering the field in respect of that part but not others such as the amendments to the Customs Act, which does not have a similar provision as proposed section 476.4? In other words, the laws are not saved; therefore, does the Cybercrime Bill in terms of its operation under the Customs Act cover the field if there were a state or territory operation? The explanatory memorandum says, in the last sentence of an explanation of proposed section 476.4:

As computer crime on internal computer networks does not involve use of the telecommunications system the Commonwealth cannot regulate this conduct.

The Australian Computer Society seemed to think that was manifestly wrong—or that the confidence may be misplaced, which, in my view, is perhaps a better way of putting it—in that the definition of 'telecommunications service' in the bill itself means 'a service for carrying communications by means of guided or unguided electromagnetic energy or both', which would mean that an internal network between two computers in a house is connected

by electromagnetic energy. Therefore, it is a telecommunications service and, as such, is caught in that sense and is not outside the process. They were both concerns that were raised in discussion with them. Did you want to deal with that?

Mr G. McDonald—Yes. Firstly, we are using saving provisions of this nature more and more to overcome difficulties where there is overlapping between Commonwealth and state laws. Obviously, I will look at the issue very carefully. However, I would think that the potential for overlap would not exist in the Customs area. However, in this area there is potential and so, just like the existing computer offences, we have exactly the same type of provision. The reason the telecommunications definition is in the Commonwealth bill is that it is related to our jurisdictional—

Senator LUDWIG—Telegraphic communications.

Mr G. McDonald—Yes. This bill is restricted to its jurisdictional environment. While you can have wires within organisations, they are still not within the jurisdiction of the Commonwealth; although, technologically, it is a little more complex than that. Sarah might have something to add.

Ms Chidgey—We sought legal advice on this matter in terms of framing jurisdiction under the bill. The advice we received was that internal networks between two computers owned by the same business, for example, do not constitute a service. That is where the difference lies: Commonwealth jurisdiction covers telecommunications services and internal networks. Our advice was that they do not constitute a service.

Senator LUDWIG—Notwithstanding your telecommunications service definition, which would then seek to include it and, then, if we stretch that to, say, a networked wireless operation—do you understand what a networked wireless operation is? Within a house you might have a wireless operation and you can network that with your neighbour, your neighbour and your neighbour, to such an extent that you have a community of wire-less operators—forgive the pun—effectively communicating in a networked fashion. Although it is without wire, certainly unguided electromagnetic energy is in use.

CHAIR—Which is what the definition says.

Senator LUDWIG—And whether or not that would—

Mr G. McDonald—That same terminology is used in the electronic transactions legislation. My understanding of it is that we have confined it to our jurisdiction, but I think we should consider that further. We will re-examine the advice and then provide you with a written comment on it. It was something about which we took advice from general counsel, and they have cleared this bill. However, as has been pointed out before, we are not perfect and so we are more than happy to do that. Obviously, this whole process is about that. We would not have this process if we were perfect.

Senator LUDWIG—I would like to balance the score. You should win one or so. In particular, I am looking at the wireless operation because they are networked now. They use clever technology, which means that they do not have to use telephone lines or ethernet cable to network. They can then use wireless technology, which could extend for quite some kilometres.

Mr G. McDonald—I have a technical expert here. The senator has made a valid point and I think we do have to take it on board.

Ms Chidgey—Their definition of telecommunications service is that it is a service for carrying communications by means of guided or unguided electromagnetic energy. This means that the definition itself is confined to a service.

CHAIR—What is a service? Where are you defining service?

Senator LUDWIG—The service could be provided by a person operating a wireless network.

CHAIR—That is exactly right.

Senator LUDWIG—So what he or she does and operates from their home is a service, and that service acts as a base—or, effectively, as an ISP—but it is not connected by cable because it is wireless. That can extend out if everyone else in the house and the neighbourhood has a wireless receiver and transmitter.

Ms Chidgey—That may be the case if one person is providing a service to other people. I think the advice we received was that, for instance, if you had a single business with computers networked on communication lines internally within that business then that would not constitute a service. But obviously if someone was providing communications networks to others then that may well constitute a service.

Senator LUDWIG—That is the group that I just mentioned. I suspect that they may not have turned their mind to the fact that there is such technology.

Mr G. McDonald—I have certainly learnt from the past. I think you gave me a twisty one on the forensic procedures bill and I thought, ‘He can’t be right on that,’ and then I went away and found out that there was a difficulty.

Senator LUDWIG—I do not wish to be right.

Mr G. McDonald—I know that. I do wish to be right on this!

CHAIR—Do you believe that, Mr McDonald? It just goes to show.

Mr G. McDonald—We will re-examine it. However, it is not something that we went into without care.

Senator LUDWIG—The other area I wish to ask you about is in relation to 3LA. There was a concern in relation to assistance from persons with knowledge of a computer or a computer system. The breadth of that was of concern. I only raise that. You may wish to then go to the submission of the Australian Computer Society.

CHAIR—Mr McDonald has undertaken to do that.

Senator McKIERNAN—I take it that despite your absence this morning and early this afternoon you have been reasonably well briefed on the proceedings to date and that you understand the thrust of the questions and areas that we have been covering during the hearing so far.

Mr G. McDonald—I was sitting down there and listening to the end of Mr Atkins’s presentation and to some of the issues.

Senator McKIERNAN—In one area that was covered there were questions about the extension of powers into the search warrants area. The last set of witnesses, the AFP, were saying that in relation to the privacy protections for those at the later parts of the warrants stream, in the networking sense, the best place to direct questions would be to the Attorney-General’s Department.

Mr G. McDonald—The situation with the privacy protections is that there have been discussions with the Privacy Commissioner's office. Certainly there is a view that with this legislation we will need to be revising the various guidelines and looking at them from a privacy perspective. That has to occur before this legislation comes into force.

You will note that the legislation has a six-month delay period before it commences, which gives everyone time not only for training but also for the development of appropriate changes to the guidelines. The specifics of the guidelines are something that I cannot tell you much about.

CHAIR—Can you give us some idea of time frame?

Mr G. McDonald—I guess the idea was that the guidelines would be developed before the legislation commences.

Senator McKIERNAN—In other words, after the passage of the bill.

Mr G. McDonald—Yes. That is certainly what we anticipated would be the case. The Privacy Commissioner is an independent statutory officer who overviews all these matters, so insistence by him of appropriate changes to existing guidelines and perhaps the development of new guidelines is something that will occur if he wants it. He certainly does want it and we and the AFP agree that you must always do that with new legislation like this.

CHAIR—The AFP have indicated that they will provide us with a copy of the guidelines they already have in place in relation to privacy protection.

Mr G. McDonald—Yes, and they may be able to give some indication of the sorts of changes that the Privacy Commissioner might like to see. Perhaps the way to go might be to talk to the Privacy Commissioner to work out an outline of the areas that might require further development. My feeling is that an outline of the areas, rather than having all the i's dotted and the t's crossed, should probably provide you with some reassurance and, as the guidelines are developed, they could be provided to you in the normal way.

Senator McKIERNAN—I am a bit surprised with your comment on the time lines. I have described the search provisions as quite dramatic. I personally still hold that view, and one of the ways that could be offset is with the development of these privacy principles. But if they are not going to be developed until after the passage of the bill, that is something that would warrant greater consideration from our point of view. But I do not have the authority to make statements on behalf of my party, so do not take that as a statement on behalf of the Labor Party or the opposition as such; it is not. It is just something I am saying on the run. But I am surprised with your comment, because I still do believe that they are quite a dramatic extension of powers. The other area that I addressed questions to is the Council of Europe Convention. Is Australia involved in those deliberations?

Mr G. McDonald—Australia has not been involved in the deliberations, except in terms of observing what is occurring.

Senator McKIERNAN—So we do have observer status?

Mr G. McDonald—We do not participate and we have not got observer status, as I understand it. By saying that we have been observing what has been happening, I mean that we have been following the development of that convention and watching what has been happening with it. As the name suggests, the convention was primarily started in Europe but there has been United States participation in the process as well. But we have not been participating.

Senator McKIERNAN—I understand it is a Council of Europe Convention. Have any of the member states of the Council of Europe initiated into their domestic laws the provisions of this convention in the draft form that it is in?

Mr G. McDonald—I think you will find that the UK, in particular, has some legislation. We can get a copy of that for you. That is one example where they certainly have new powers in this area that are similar to the sorts of powers talked about in the convention. In relation to other European countries, we could provide some additional material. I am aware that the UK and the US have substantial powers.

Senator McKIERNAN—Is the US a formal part of those convention proceedings?

Mr G. McDonald—Yes, that is correct.

Senator McKIERNAN—Is that unusual? I do not want to get into a debate on that.

Mr G. McDonald—No. The thing that surprised me in the context of other matters that I have been participating in is this concept of having an organisation doing a lot of work and then involving other countries. That seems to be happening quite a lot where the countries have a similar interest. For example, I have been involved in the OECD bribery of foreign officials process. The OECD have 30 countries, or thereabouts, and they have been evangelising. There are quite a number of countries coming in and taking up the OECD convention, and the OECD are actively going out and getting more countries to become involved. I would say that the Council of Europe process was probably already under way and, with increasing global problems in this area, other countries have become involved.

Senator McKIERNAN—Another area we discussed earlier today was the lack of definitions contained in the legislation—in particular, no definition of a computer and no definition of what a computer network is—and asking those question in light of the advice from the officers' group that there be no definition. I put it to one of the earlier sets of witnesses that there will ultimately be a definition made by the judiciary and is it not putting us, as legislators, in a position where we are abdicating our responsibilities. It is our responsibility, as legislators, to determine the law and the responsibility of the judiciary to implement it. Are we not being put in a position where we are abdicating our responsibilities by not including in this legislation a definition of those two key factors, at least—that is, what is a computer and what is a computer network?

Mr G. McDonald—The view of all the people from the various states and territories, certainly our view and the view from what we have seen in many other places is that this is one area where it is far better not to have a technical definition. The technology is moving so quickly that even the provisions we enacted in 1994 are looking like ancient history. The courts, of course, as with other areas, can get expert advice or expert witnesses to inform them on the latest technology rather than being in a position where they are continually trying to develop another definition of 'computer'. I think Stephen was mentioning this morning about the Council of Europe's effort. Perhaps I am wrong, but there were some efforts in the past that were quite—

Senator McKIERNAN—He is a bit foggy about that one!

Mr G. McDonald—Foggy is right!

CHAIR—Perhaps you can come back to us on that point, Mr McDonald?

Mr G. McDonald—Yes. But there have been problems with definitions being out of date before they got royal assent.

Mr Orłowski—Certainly the definition we would have applied in 1988—at that time there was a conscious decision not to include a definition—would have been completely irrelevant today, and 99 per cent of offences would not have been able to be prosecuted because they were occurring outside what was then considered to be a computer.

Senator McKIERNAN—I accept that, but has that lack of definition in that period of time caused any problems in the sense that the judiciary had to make a definition or come to some understanding of what computers were?

Mr G. McDonald—I am unaware of any problems.

Senator McKIERNAN—The figure of \$3 trillion was mentioned in the second reading speech. What was the source of that figure?

CHAIR—It is at the end of the first paragraph of the second reading speech.

Ms Chidgey—It was from a news report, Senator McKiernan. It was an estimate provided by the United States National Security Agency.

Senator McKIERNAN—Can you give us a bit more evidence than that?

Ms Chidgey—We can follow it up.

Senator McKIERNAN—Are there any figures on the estimated costs within Australia? I see, that was a worldwide figure. Incidentally, what is a trillion?

Mr G. McDonald—It is 3,000 million if you want to use the English system.

Senator McKIERNAN—Is that more than a billion?

Mr G. McDonald—I think I need an expert on maths here.

CHAIR—It is a lot.

Senator McKIERNAN—We will ask Finance. Is there any estimate of what the current cost to Australia is?

Mr G. McDonald—I have no idea.

Senator McKIERNAN—Is there any estimate of the number of crimes being committed in Australia that would come under the umbrella of this legislation?

Mr G. McDonald—That would be impossible to estimate in relation to any theft, fraud or drugs in this area. The interesting thing about crime trends, statistics and so on is that so many factors can come into them. Some of the questions you asked earlier are almost impossible to answer. I mean, Senator Ludwig asked the AFP, ‘How many more would you prosecute if this went through compared to sticking with the existing law?’ It ends up simply being informed guesstimates at the best, except to say that with this legislation we have identified areas where existing law can be improved, areas which were uncertain or areas which were simply not covered and which are things that can do harm. So it is quite clear that by putting these laws in place there will be more people who could be prosecuted.

Mr Orłowski—Two surveys have been conducted, one by the Office of Strategic Crime Assessments and the Victorian police in 1997 and one by Deloitte Touche Tohmatsu in 1999, which addressed the issue of what sorts of crimes were being experienced by business, as opposed to individuals. We could certainly get you copies of those two studies.

CHAIR—Thank you, that would be helpful.

Mr G. McDonald—I think there may be some material as well in the ABCI material that I gave you which would be worth looking at.

Senator McKIERNAN—We have not actually got on top of that material yet, would you believe?

Mr G. McDonald—I know.

CHAIR—It has been very slow this afternoon.

Senator McKIERNAN—It is very important legislation.

Mr G. McDonald—Yes.

Senator McKIERNAN—The onus is on us to get it as right as possible at this time, recognising that there will be modifications needed down the line, hence the reason for asking the questions. Even informed guesstimates or references to articles that appear in newspapers can be of assistance, especially if they are good enough to be used in the second reading speech by the Attorney-General.

Mr Orłowski—If you are interested in trends analysis of what has been happening, the AusCERT web site has figures broken down over the years.

CHAIR—Okay. We had a reference to AusCERT earlier, so we can pursue that. As there are no further questions, thank you, Mr McDonald, Mr Orłowski and Ms Chidgey, for your assistance this afternoon. I would like to thank all of the witnesses who have given evidence to the committee today and also of course the secretariat and *Hansard* for assisting the committee with our deliberations. We intend to hold a further public hearing on this piece of legislation, almost definitely to be held in Canberra. Advice of that will be made public when it is determined. I declare this meeting of the Senate Legal and Constitutional Legislation Committee closed.

Committee adjourned at 3.55 p.m.