COMMONWEALTH OF AUSTRALIA

Proof Committee Hansard

JOINT SELECT COMMITTEE ON CYBER-SAFETY

Cybercrime Legislation Amendment Bill 2011

(Public)

MONDAY, 1 AUGUST 2011

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

[PROOF COPY]

INTERNET

Hansard transcripts of public hearings are made available on the internet when authorised by the committee.

The internet address is:

http://www.aph.gov.au/hansard

To search the parliamentary database, go to:

http://parlinfo.aph.gov.au

JOINT SELECT COMMITTEE ON CYBER-SAFETY

Monday, 1 August 2011

Members in attendance: Senator Bilyk and Mr Hawke and Ms Marino.

Terms of reference for the inquiry:

To inquire into and report on:

Cybercrime Legislation Amendment Bill 2011

WITNESSES

BUDAVARI, Ms Rosemary, Co-Director, Criminal Law and Human Rights, Law Council of Australia..... 1

CHIDGEY, Ms Sarah, Assistant Secretary, Criminal Law and Law Enforcement Branch, Criminal Justice Division, Attorney-General's Department..... 23

CLARKE, Dr Roger, Chairman, Australian Privacy Foundation and Privacy International..... 6

CONNOLLY, Mr Chris, Research Associate, Cyberspace Law and Policy Centre, University of New South Wales..... 12

CRAMSIE, Mr David, Senior Legal Officer, Telecommunications and Surveillance Law Branch, Attorney-General's Department..... 23

FRICKER, Mr David, Deputy Director-General, Australian Security Intelligence Organisation..... 23

FROELICH, Mr Peter Anthony, Principal Domain Expert, Telstra Operations, Telstra..... 17

GAUGHAN, Assistant Commissioner Neil, National Manager, High Tech Crime Operations, Australian Federal Police..... 23

KILEY, Mr Andrew, Senior Legal Officer, International Crime Cooperation Division, Attorney-General's Department..... 23

SENGSTOCK, Ms Elsa, Coordinator, Legislation Program, Australian Federal Police..... 23

SHAW, Mr James, Director, Government Relations, Telstra..... 17

SMITH, Ms Catherine, Assistant Secretary, Telecommunications Surveillance Law Branch, Attorney-General's Department..... 23

VAILE, Mr David, Executive Director, Cyberspace Law and Policy Centre, University of New South Wales..... 12

WATERS, Mr Nigel, Board Member, Australian Privacy Foundation and Privacy International..... 6

BUDAVARI, Ms Rosemary, Co-Director, Criminal Law and Human Rights, Law Council of Australia

Committee met at 10:24

CHAIR (Senator Bilyk): I now declare open this public hearing of the Joint Select Committee on Cyber-Safety of the Commonwealth parliament for its inquiry into the provisions of the Cybercrime Legislation Amendment Bill 2011. Today the committee will be hearing from the Law Council of Australia, the Australian Privacy Foundation, the Cyberspace Law and Policy Centre, and Telstra. The Cyberspace Law and Policy Centre will give evidence by teleconference; all other witnesses will appear in person. After a short lunch break, the committee will hear from the Attorney-General's Department, the Australian Federal Police and ASIO together. After the hearing, members will conduct a site inspection of the AFP High Tech Crime Centre in Barton. This is a public hearing of the inquiry and is being broadcast live. The transcript of today's proceedings will be posted on the committee's website.

I welcome our first witness. Although the committee does not require you to speak under oath, you should understand that these hearings are formal proceedings of the Commonwealth parliament. Giving false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. I remind you that the hearing is public and is being broadcast live. I ask you to make a short introductory statement; the committee will then proceed to questions.

Ms Budavari: The Law Council of Australia has made a submission on a discrete part of the bill that is the subject of the committee's inquiry. That submission deals with schedule 2 of the bill. Schedule 2 deals with the disclosure of information to assist in the investigation by foreign countries of serious contraventions. The disclosures in schedule 2 are made pursuant to stored communications warrants or authorisations relating to telecommunications data. The Law Council understand that the committee will be hearing from the Australian Privacy Foundation and the Cyberspace Law and Policy Centre in relation to the bill more generally, so we wish to confine our comments to schedule 2. We also understand that the committee has heard from the Ombudsman's office, which has an existing role in relation to examining reports relating to stored communication warrants and authorisations relating to telecommunications data purely in the domestic context.

In relation to stored communications warrants and authorisations relating to telecommunications data to assist in investigations by foreign countries, the explanatory memorandum to this bill notes that the bill seeks to implement articles 30, 31 and 33 of the Council of Europe's Convention on Cybercrime. Article 31 provides for access for foreign countries to stored computer data. Article 30 provides for disclosure of traffic data—or telecommunications data, as we would put it—to foreign countries to enable the identification of service providers and the path of a communication. Article 33, importantly, provides for mutual assistance to foreign countries regarding real-time telecommunications data. None of those articles from the convention specifies a particular process to be adopted by the country providing the data. Article 33 in fact refers to the mutual assistance being governed by conditions and procedures provided for under domestic law. In the Law Council's view, it is important that the committee consider what the existing domestic procedures are and whether there is justification for departure from those domestic procedures in the context of disclosing information to foreign countries.

Having said that, the Law Council does not object to Australia's implementation of this convention, nor to the facilitation of provision of information relating to stored communications and telecommunications data. But the Law Council considers that some of the proposed provisions in schedule 2 are drafted too broadly and that there are some significant omissions in how the articles are being implemented. In this regard we have suggested some alternative provisions in our submission for the committee to consider. The Law Council has previously made submissions on amendments to the telecommunications legislation and the mutual assistance legislation being considered here, which have emphasised the need for appropriate safeguards to be included in this legislation. In relation to the telecommunications legislation the Law Council has in the past stressed and continues to stress that the primary object of that legislation is to prohibit interception and access to communications, stored communications and telecommunications data. Every exception to this general prohibition needs to be carefully scrutinised by parliament to ensure that it goes no further than necessary.

Similarly, in relation to the mutual assistance legislation, every response by Australia to a request for assistance has significant consequences either for an Australian or for a person in a foreign country who are being investigated for or who have been charged with criminal offences. Any expansion of the powers under this legislation also needs to be carefully scrutinised, whether it be in the context of cybercrime or any other context.

The first issue we have addressed in our submission is the definition of a 'serious foreign contravention', to which the investigation in a foreign country must relate for a stored communication warrant to be issued. The bill

proposes to insert a new definition into section 5E of the Telecommunications (Interception and Access) Act, which defines the serious foreign contravention by reference to a penalty of three years imprisonment or more, or 900 penalty units, but under the law of the foreign country not under domestic Australian law. It is consistent with the penalty threshold for stored communications warrants for domestic offences but, in the Law Council's view, it is likely that foreign countries may, in some instances, have higher penalties for similar offences and that effectively lowers the threshold for the issue of the stored communications warrant for foreign offences. We have submitted that the relevant provisions should be amended to require that the foreign offence under investigation would attract the requisite penalty had it been committed in Australia.

We note in this regard that one of the relevant statistics that the amendments to the bill require to be reported on in the minister's annual report to parliament on stored communication warrants will be the similarities between the foreign offence and the relevant domestic offence. If that is going to be reported on at the end of the process, the Law Council argues that it can also be considered at the beginning of the process and that there can also be a comparison of the penalties.

The Law Council also notes that a number of details about the request need to be provided in the mutual assistance application, which was initially made under section 8 of the Mutual Assistance in Criminal Matters Act and that it should not be impossible for that application to compare the relevant domestic and foreign offence and the penalties as well. It may be that the Attorney-General's Department can provide some insight into why that suggestion has not been taken up, because it has been raised with the department previously. But, in the absence of access to the Attorney-General's Department's submission, the Law Council is not in a position to assess whether there is sufficient justification for that. The second issue that we have addressed in our submission is the proposed amendment to proposed section 116 of the Telecommunications (Interception and Access) Act, which provides for different considerations by the issuing authority of a stored communications warrant in the case of a mutual assistance application relating to investigation by a foreign country and that the considerations for that application will be different from the considerations for a stored communications warrant in the domestic context.

In that regard, the Law Council notes a number of the considerations for the issuing authority in the domestic context, such as: to what extent the methods of investigating the relevant offence that do not involve the use of a stored communications warrant have been used by the agency seeking the warrant; how much the use of such methods would be likely to assist in connection with the investigation by the agency of the relevant offence; and how the use of such methods would be likely to prejudice the investigation by the agency of the serious contravention. Those three considerations are not present in the considerations that need to be weighed by the issuing judge or member of the AAT in relation to a stored communications warrant that has been requested by a foreign country.

In the Law Council's view, again, there is no justification given in the explanatory memorandum for why there is a difference in this particular case. The third issue that the Law Council has raised—

CHAIR: Sorry to interrupt; we have the ABC here. I wonder whether you have any concerns about being filmed.

Ms Budavari: No, that is fine. I will try to wind up.

CHAIR: No, that is fine. I did not mean to throw you off track. I just needed to clarify that.

Ms Budavari: That is completely fine. The third issue that the Law Council has raised is in relation to the different reporting requirements for stored communications warrants in the domestic context and those which have been issued for matters relating to foreign countries. In that regard, what appears to have been omitted is any requirement to report on the number and type of arrests made, prosecutions instituted and convictions secured as a result of the information obtained under the warrant. Once again, the Law Council recognises that it can be difficult to obtain this sort of information from foreign countries. But if foreign countries want to obtain the relevant stored communications information from Australia, we consider it is reasonable to ask them to reciprocate with this type of information so that the Australian authorities can assess whether it was actually justified to release that information to the foreign countries.

The fourth issue that the Law Council has raised in the context of stored communications is the enforceability of any conditions imposed on the disclosure of the information which is authorised by that warrant. These are set out in proposed section 142A. The Law Council agrees with those conditions. We consider that those conditions are appropriate. The concern we are raising is how they will be enforced. We suggest that perhaps proposed subsection 8(2) of the mutual assistance act should be amended to insert an additional discretionary ground for refusing a mutual assistance request, which would encourage the Attorney-General to decline a request for assistance where the requesting country's arrangements for handling personal information do not abide by those

conditions relating to the destruction of the information when it is no longer required and the information only being used for the purposes for which the foreign country has requested it. If those conditions are not abided by, the Attorney-General actually has a discretion in future instances to decline a request for assistance from that country.

Turning to the other major area that is dealt with in schedule 2, the area of authorisations to disclose telecommunications data. This does not require the issue of warrants. In the domestic context it can be done by authorised officers provided certain conditions are met. In the domestic context there are stricter requirements for the disclosure of telecommunications data, which is labelled either 'historical' or 'existing' then there is for the disclosure of prospective data—what we would call real-time data. This distinction has been transferred to the proposed amendments so that the requirements for the disclosure of real-time data are stricter in the context of a request by foreign country for access to that data.

That is commendable. However, the Law Council is concerned that there is a very broad test proposed for determination by an officer of a criminal agency of when to authorise disclosure of either historical or prospective data in the bill. That test is that:

> ... the disclosure is reasonably necessary for the enforcement of the criminal law of the foreign country and the disclosure is appropriate in all the circumstances.

In the Law Council's view that requirement that the disclosure is appropriate in all the circumstances is far too ambiguous to act as an effective safeguard. It provides little guidance to the relevant officer about the types of matters that the legislature intends that he or she will consider before authorising the disclosure.

In that regard, the Law Council is suggesting to the committee that it considers that the bill should be amended to provide that, without limiting that relevant provision, in determining whether a disclosure is appropriate in all the circumstances, the authorising officer has to give consideration to the mandatory and discretionary grounds for refusing a mutual assistance request that are listed in section 8 of the Mutual Assistance Act. Section 8 of the Mutual Assistance Act sets out a wide range of considerations, most of which will not come into play in the cybercrime context. Section 8 of the Mutual Assistance Act deals with providing assistance in cases where there are political offences or a person may be subject to the death penalty. That is probably not going to come into play in a cybercrime context. But it also allows the Attorney-General in mutual assistance requests to look at factors such as—and this is in a discretionary context—whether the request relates to the prosecution or punishment of a person in respect of an act or omission that if it had occurred in Australia would not have constituted an offence against Australian law, or whether the provision of the assistance would prejudice the safety of any person whether within or outside of Australia, or whether the provision of the assistance would impose an excessive burden on the resources of the Commonwealth or the state or territory. So it sets out a number of more clearly defined considerations for someone to assess whether the disclosure is appropriate in all circumstances. The Law Council commends that type of model to this committee.

Finally, the Law Council's submission also raises the issue of how the proposed conditions relating to the disclosure of telecommunications data to a foreign country will be enforced without some form of undertaking given by a properly authorised person from that country to abide by those conditions. Again, the Law Council considers that the conditions that are set out in the bill are appropriate, but once that information leaves Australia, how Australia ensures that those conditions are met is an issue. It may be that the Attorney-General's Department or the AFP can address some of those concerns to the committee's satisfaction. But in the absence of access to the Attorney-General's Department's submission, the Law Council simply raises these matters for the committee's consideration. That includes my opening statement and I am happy to answer questions.

CHAIR: Thank you for your comprehensive opening statement. Mr Hawke has questions.

Mr HAWKE: You have raised quite a lot of concerns in reality about how some of this would operate in terms of telecommunications interception. I want to begin with the categories of offences in relation to foreign powers and Australian law. You have raised a series of things here which I think are quite valid: political offences; things that are not offences in Australian law; and punishing people on the basis of various categories of race, religion and other things. Have you considered issues such as civil and criminal law? Some countries have things in their criminal law that are only civil offences in Australia. Have you thought about that issue or how that would work? One that has been raised with us, which I have a particular interest in, is copyright law, which in some countries is a criminal matter but in Australia is a civil offence. Have you thought about that from your point of view?

Ms Budavari: We have not really considered that. It is probably important to note that the Mutual Assistance Act which will govern the stored communications warrant regime and the prospective telecommunications data regime—so for both of those there has to be a mutual assistance request first—does in fact require that the request

relates to the prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Australia, would have constituted an offence against Australian law. That is the kind of dual-criminality point that is raised by the bill. But certainly in relation to the matters which relate to stored communications warrants and disclosure of prospective telecommunications data it would appear that the requirement would be that whatever the serious foreign contravention is that is actually an offence against Australian law as well.

Mr HAWKE: Okay. But you do not think the dual criminality requirement is sufficient, which was the basis of what you were saying before about dual criminality?

Ms Budavari: There needs to be dual criminality, yes.

Mr HAWKE: Yes, in all cases.

Ms Budavari: Yes.

Mr HAWKE: With the stored communications data, we have also had it raised to us about 90 days with carriers. Does the Law Council have a view about this bill in terms of what would happen to that information in the hands of carriers? The bill at the moment, it has been pointed out, is silent about what would happen to that information being held by carriers after 90 days. Agencies are required to destroy it under the current acts and under the proposed amendments. Have you examined that issue?

Ms Budavari: We have not really looked at that issue specifically. Yes, I probably cannot assist you with that particular one, unless we took it away and have a look at that.

Mr HAWKE: Do you have concerns about the length of time in relation to either the stored Communications or the prospective warrants being 29 days and 90 days, respectively? Do you have concerns about the length of time of the operation of those clauses?

Ms Budavari: Again, we probably cannot comment on the length of time, because we really have not looked at the actual operation of these things within the domestic context in terms of time. I would assume that the ombudsman's office has perhaps looked at that—or certainly the Attorney-General's Department would have data, presumably on that. They may be able to assist you with that.

Mr HAWKE: In relation to this entire suite of legislation, with telecommunications interception and the application of domestic preservation orders, have these matters been tested in court to your knowledge in terms of agencies applying for these? Are there any notable cases you are aware of where this has been put to court in terms of their legality or otherwise in accessing carrier information?

Ms Budavari: I am not aware of any particular cases. Again, that would probably be something we would need to look at.

Mr HAWKE: Does the council have any concerns about the legality of the operation of these provisions?

Ms Budavari: Certainly in the domestic context these provisions have been operating for some time, and there are annual reports to parliament. Sometimes those reports raise some issues about the operation—some systemic issues that then appear to be addressed by the agencies. But the Law Council has not looked closely at each of those reports. We have certainly looked at the most recent report, and there were some issues raised in that with the use by the Australian Crime Commission of some of these interception warrants and stored communications warrants that appear to be being addressed.

Mr HAWKE: So, on the issue of carrier handling of data, you have not really got a strong view about that and the operations at all?

Ms Budavari: No.

Mr HAWKE: Thank you for that.

CHAIR: Before I go to Ms Marino, I have a point of clarification. Can you tell the committee whether dual criminality applies to police-to-police assistance as opposed to requests under mutual assistance?

Ms Budavari: I cannot tell the committee off the top of my head, but certainly there are guidelines. The Law Council has looked at the relevant guidelines for agency-to-agency assistance in death penalty cases, and obviously there is a requirement for dual criminality in that context, but we have not looked at the issue more broadly.

CHAIR: Thank you. Historic and existing telecom data does not require a mutual assistance request, does it?

Ms Budavari: No, it does not.

CHAIR: Thank you.

Ms MARINO: Thank you very much. One of the things that the Law Council touched on was the fact that there is no proposal within the bill to restrict the information to the countries that are signatories to the European convention. Is it the view of the Law Council that that the access should be restricted to those countries?

Ms Budavari: I am not sure that we raised that particular issue, but it is obviously an issue. We have not actually looked closely at the requirements of the convention in that regard. We could certainly do that and come back to the committee.

Ms MARINO: I would be interested in your comments about that. I think that one of the things that you touched on or that were in the submission was the fact that the bill is silent on this and does not restrict it to those countries. I would be interested in your view on that. Also, you touched on the issue of what happens to the information—how it is handled and the fact that the Attorney-General should perhaps consider not having further dealings with a country that does not comply. In relation to the actual compliance in those other countries, does the Law Council have a view on what further things could be in this bill that would assist in managing that issue?

Ms Budavari: One of the things that we suggested in the submission is that an undertaking be sought by an appropriately authorised officer of the country. Again this has arisen in the context of our work on death penalty cases. In those cases it is often the case that the government will seek an undertaking that the death penalty will not be imposed before providing assistance. In that context, we have been quite concerned to ensure that the official who gives that undertaking is appropriately authorised to do that. This is a very different context, but you could in fact use the same sort of model of a safeguard. So you would be requiring a country to give an undertaking that those conditions will be abided by and requiring that undertaking to be given by someone with sufficient authority to give it. So it would not be a low-level official but someone, in our context, probably at departmental secretary level or even ministerial level who would be required to give that undertaking.

Ms MARINO: I have one other issue and I do not know if you have given it any consideration but the information coming from carriers would need to be copied. Does the Law Council have any view on what would happen to that information? How long would it need to be before that information was destroyed and what process should be used to ensure that it happens?

Ms Budavari: There are provisions in the existing telecommunications legislation for revocation of authorisations when the information is no longer required by the particular agency. Yes, we would want to see adherence to those provisions which provide for revocation and strict requirements for revocation once the information is no longer required.

CHAIR: The Law Council has criticised the proposed new section 180F of the Telecommunications (Interception and Access) Act 1979 because it merely requires an authorising officer to 'have regard' to the privacy of the person whose communication data is to be revealed. Can you explain to us why it appears that the terms 'have regard' are insufficient for you?

Ms Budavari: I think you will find that one of the suggestions we have made is that there be something a little stronger in that context. The suggestion is that the relevant section be strengthened to read something like, 'Before making an authorisation, an authorised officer must be satisfied on reasonable grounds that the likely benefit to the investigation which would result from the disclosure substantially outweighs the extent to which the disclosure is likely to interfere with the privacy of any person or persons.' It would put a kind of proportionality type of test in there rather than just a simple reference to 'consider the impact on the privacy of a person.'

CHAIR: Would that not happen, though, through the process of seeking a warrant?

Ms Budavari: Not necessarily. This section is in the context of the authorisation of telecommunications data, so you are not actually seeking a stored communications warrant in this context. You have an officer of an agency who is making this assessment rather than a judge or a member of the Administrative Appeals Tribunal. We are simply saying that the more guidance you can give that officer the better, to ensure that those safeguards are adhered to.

CHAIR: Thanks for clarifying that. Thanks for your evidence today. It has been a valuable contribution to the inquiry.

Proceedings suspended from 10:58 to 11:11

CLARKE, Dr Roger, Chairman, Australian Privacy Foundation and Privacy International

WATERS, Mr Nigel, Board Member, Australian Privacy Foundation and Privacy International

CHAIR: Welcome. Although the committee does not require you to speak under oath, you should understand that these hearings are formal proceedings of the Commonwealth parliament. Giving false or misleading evidence is a serious matter and may be regarded as contempt of parliament. I remind you that the hearing is public and is being broadcast live. I ask you to make a short introductory statement and the committee will then proceed to questions.

Dr Clarke: Thank you. I will briefly make some comments about some procedural aspects relating to the bill and my colleague will then address the substantive aspects. The process that surrounded the review of the legislation by this committee has been in direct conflict with the reasonable expectations of civil society. The time set was ridiculously short, as we have explained in our submission—originally five business days and at the end of those five business days an extension of a further seven. This makes it extremely difficult for public interest advocacy organisations because they depend almost entirely on the unpaid time of busy professionals working in various locations across the continent. A further impact of the unseemly haste has been that even as late as 8 am this morning the submissions to the committee were still not publicly available and we only know of a few of the organisations that have submitted. This makes it impossible for witnesses to appreciate the perspectives of other interested parties.

A third concern is the failure of the proponents of the bill to provide a document tracing the long history of the cybercrime convention and the government's response to it. This concern is compounded by the fact that this bill extends well beyond its nominal purpose to the further detriment of human rights. The fourth process issue is that no consolidated statutes of been provided to assist in understanding the impacts of the amendments.

This is a joint committee and it has an opportunity not available to committees of a single house. We submit that your committee must grasp the opportunity to force the proponents of bills into the late 20th century. You should require proponents to make available meaningful background information and copies of consolidated legislation and you should make clear to both chambers that a clear 25 working days notice is essential for the receipt of submissions prior to hearings commencing.

Mr Waters: I would like to start by saying that the Privacy Foundation is sympathetic to the stated objective of this bill and that we consider that mutual assistance and cooperation is desirable to combat the problems of some types of cybercrime, including aspects of cybercrime that go directly to issues of privacy. So we have a common interest with the proponents of the bill in seeing appropriate forms of law enforcement.

The cybercrime convention itself was very controversial when it was being drawn up in the early part of this century. Civil society had significant concerns and also had significant influence in the development of the cybercrime convention in its final form. However, it is still, in our view and in the view of NGOs around the world, significantly flawed. This bill, in our view, goes well beyond what is required for mere accession to the cybercrime convention and is being used as an opportunity by the law enforcement community to get access to powers which they have been looking for for some time. This is just another opportunity for an ambit claim.

We think it is important that the committee understand some of the context in this area, particularly since, in the past, issues of interception and access have been handled by the Senate Legal and Constitutional Affairs Committee, so this committee does not have the corporate memory that that committee would have if they were looking at the bill. Aspects of that context include the fact that communications are increasingly, in the modern age, moving from real-time into stored communications and also the fact that traffic data is nowadays much more revealing about individuals' communications than it used to be. In the old days it was simply who phoned what number at what time. Now the traffic data, particularly in relation to internet use, is potentially much more revealing of the content of individuals' communications or the likely content of it and therefore the strict rules that apply at the content end under the interception regime do not apply at the traffic end of the spectrum. Yet increasingly we are seeing law enforcement agencies seeking powers to enable them to access traffic data and the intermediate category of stored communications data. Traffic data, we point out, is not subject to a warrant regime, so the assertion in the explanatory memorandum that we should be satisfied by the fact that there will eventually be a warrant application is misleading, because that does not apply in the case of traffic data.

The other bit of context is that warrants are available both for content and for stored communications now to many more agencies than used to be the case for a wider range of offences than used to be the case and that

warrants are now predominantly issued by members of the Administrative Appeals Tribunal rather than judges. With due respect to the AAT members, they are simply not in a position to be as independent of the executive as judges were when they were the only parties able to issue warrants. Another bit of context is that there is a higher incidence of interception in Australia on a per capita basis than almost anywhere else in the world, including the United States. So these powers to intercept and access communications are being used disproportionately more in Australia. There is also a significant element of both cost shifting to the private sector, which reduces the barrier effect to law enforcement and makes them more likely to seek access than when they had to pay significant costs for interception. The general effect of the trends in the regime have been to effectively deputise the private sector to perform the functions and bear the costs that were previously borne by law enforcement. We think those are important areas of context.

In relation to the provisions of the bill, we have many significant concerns, which are set out in our submission. Those that relate to two very significant areas I am not going to dwell on because they are covered extremely well in the other submissions which I understand you have received from the councils for civil liberty. Those are in the areas of the definition of cybercrime. I think there is a consensus amongst all civil society organisations that the definitions in this bill are far too broad. The other area is dual criminality—the lack of a requirement in the legislation for offences to be a crime under Australian law in order to trigger the provisions of preservation orders and subsequent access by foreign governments. I will briefly touch on our concerns and our recommendations in relation to the other areas. These are covered in section 5 of our submission, specifically subsections 5.1.1 through to 5.4. Firstly, we have concerns about the definition of 'telecommunications data', and its relationship to the definition of 'stored communications'. We think that this bill significantly muddies the water when it comes to that important distinction in a way that departs from the existing distinction between content and stored communications data in the existing Telecommunications (Interception and Access) Act regime. It is important that those definitions are made clearer and that the intent of the bill is made clear in relation to the different categories of information.

Secondly, we have a major concern about the definition of 'telecommunication services'. We fear, although it is very difficult from the material provided to be certain, that this may provide a backdoor for law enforcement agencies to seek access to bulk stored communication data and traffic data, which would take it into the area of data retention which, as the committee may know, is a very controversial area that the government has been consulting on behind closed doors to date—although I think the government has announced that it will be bringing forward proposals for a data retention regime in the near future. But it is important, in our view, that the committee seeks an explanation about the government's intentions in relation to retention versus preservation, which has been a very controversial debate, particularly in Europe.

We have concerns about the breadth of the definition of 'issuing agency'. Our reading of the bill is that preservation orders are going to be able to be sought and issued by a wide range of agencies, not just those that you might traditionally regard as the primary law enforcement agencies. We have very significant concerns about the scope of the bill in relation to the term 'foreign countries', and in particular we call on the committee to ensure that the foreign countries that are able to take advantage of the provisions of the bill must be limited to those which have adequate protection for human rights and civil liberties.

There is no vulnerability test, as far as we can see. In other words, preservation orders will be able to be issued whether or not there is any likelihood of the data being disposed of, which seems like an overreaction and will lead to an unnecessary volume of preservation notices. There are no specific security or integrity obligations, and while the security requirements and the data quality requirements in the various privacy laws may apply in some cases to some of the agencies concerned, we think that is not good enough and that there should be specific obligations in this bill if it was to proceed. The relationship to data retention I have already mentioned and we deal with that specifically in 5.3.

In 5.4 we set out a number of concerns about the inadequacy of privacy protections in the bill, specifically the need for a better balance within the bill itself between the coercive powers and other protections. The cybercrime convention itself seeks to strike that balance, and has various clauses which suggest that there should be countervailing human rights protections, but it also defers to the fact that all of the Council of Europe parties, or all of the European parties to the convention, are also subject to the Convention on Human Rights, and that is a gap in the Australian context which needs to be balanced in the absence of any general human rights legislation or constitutional rights to privacy by specific provisions in the bill.

There is a meaningless privacy test that, on the face of it, looks good. Basically it requires authorising officers to have regard to privacy, but there is no real way of ensuring that they take any notice of privacy or get the balance right. We believe that should be pinned down to ensure that there is a proportionality requirement that

requires a balance between privacy and the interests of the law enforcement agencies. It is important to note that that privacy test applies to both the issuing of preservation notices and also to subsequent applications for access to resulting data. We have concerns about the extent of delegation to the authorising officers, very significant concerns about the inadequate oversight of the whole regime. We find it disappointing that the ombudsman's evidence was apparently given in camera this morning. While there may be some sensitivities around particular issues, we cannot for the life of us see why the ombudsman would not be prepared to discuss in public the general oversight regime. We strongly endorse—although this is not in our submission—the views of the Queensland Council for Civil Liberties in recommending the introduction of a public interest monitor role in relation to this and other legislation.

We have concerns too about identity standards so that individuals are not wrongly targeted, concerns about secondary use limitations and in particular the enforceability of the limitations which are incorporated in the bill, and very significant concerns about the cross-border disclosure regime where there appears to be no way of guaranteeing or enforcing limitations that are supposedly placed on overseas law enforcement agencies who are in receipt of any data resulting from this regime.

Finally, we would like to draw attention to our concerns about the excessive confidentiality requirements—this is in section 6 of our submission. We believe there should be a prejudice test; in other words, that it should be possible for individuals to find out that their communications have been subject to a preservation order or disclosed to law enforcement agencies once there is no longer any prejudice to an ongoing investigation. We also would like to see a proactive notification regime such as applies in the United States in relation to wire taps once there is no longer any prejudice to an investigation. So overall we would like to see a much greater degree of transparency and in particular the rights of individuals to find out that they have been subject to this regime.

I would like to summarise our overall views as set out in section 8 of our submission. We believe the bill has been placed before the parliament in a manner that obstructs understanding of its meaning and analysis of its impacts. The bill seeks to impose all of the intrusive elements of the convention without allowing for the convention's presumption that strong human rights protections are in place. As a result, the provisions would create grossly unbalanced and excessive legislative powers. Despite its claimed purpose, the bill goes well beyond what is necessary in order to accede to the convention and the extensions are highly privacy abusive. Despite the barriers to understanding, the APF has identified 16 serious features which should under no circumstances be passed into law. The bill very probably contains further excessive features which cannot be readily detected because of both the inherent and the contrived complexities in the material provided to date. The privacy foundation submits that the committee must find that in its present form the bill is completely unacceptable and incapable of sensible amendment into an acceptable form and should be sent back to the department for further work.

CHAIR: Thank you. In regard to Dr Clarke's comments, the committee has received 22 submissions and today they are being put up on the web, as I understand. This is an extra committee for the purposes of looking at this legislation, so this is not what would normally be the process. We did listen to the concerns about the time frame and did extend as far as we could. I do not want to be churlish about it and I want to point out those things to you. Also the inquiry is into more than just cybercrime. Before I hand over to other members, can you distinguish for me between traffic data and content data and what your definitions are?

Mr Waters: Yes. At the moment, between the Telecommunications (Interception and Access) Act and the Telecommunications Act is created a tripartite distinction. Firstly, there is what is called 'substance and content of communications' which is real-time, typically, voice content while a communication is taking place. Secondly, there is a concept of stored communications, which was introduced a few years ago to deal with things like message banks, SMS, text and email, which is stored and forwarded. So it exists for a period of time before individuals typically access it and read it, and then decide what to do with it. Then there is a third category of information which is covered by a separate regime in those acts which is all other telecommunications data, including customer subscriber details but also traffic data such as things like who dialled what number at what time. That is a very important distinction which is sort of addressed reasonably well in the existing legislation. Our reading of this bill suggests that it confuses stored communications and traffic data, and subjects both of them to some weaker protections than currently exist.

CHAIR: Can you expand on your concerns about Australia's accession to the convention in relation to protecting intellectual property rights?

Mr Waters: That is an area that one of our other colleagues is particularly knowledgeable about and which I would probably have to take on notice. The general point is that we see an increasing trend to intellectual rights' holders seeking to take action against people whom they suspect of breaching their copyright, particularly in

relation to internet use, and seeking to engage provisions in the criminal law in different jurisdictions in order to pursue those people. We do not think it is appropriate to deal with that whole issue in the same way as you deal with serious crimes, terrorism and the various other offences for which interception and access regimes have typically been put in place. We see an increasing trend towards, in a sense, commercial interests riding on the back of very significant public interest powers that have been given for much narrower purposes.

CHAIR: Thank you.

Ms MARINO: You touched on the fact that you believe that we should only be accepting requests from countries that have a strong human rights background. Would that mean that we would only accept requests from countries that are part of the convention, in your view, or would it be different to that?

Mr Waters: Not necessarily. There are countries that have not acceded to the convention which do have very strong human rights protections, and that may be because they have not yet got around to acceding to the convention or it may be because they have some objections based on our objections to the convention. The important thing is to ensure that there are some appropriate criteria for human rights protections at all the different stages—applying for a preservation order then subsequently seeking access and then getting mutual assistance under various arrangements with our law enforcement agencies.

Ms MARINO: You touched on the issue of disclosure afterwards to an individual who has had their records accessed. What redress do you see for those whose personal data has been accessed and who have been wrongly accused as a result of this type of thing?

Mr Waters: In many cases, it may well be that there were reasonable grounds for them being under suspicion and then subsequently they were found not to be a subject of interest. We do not think that that necessarily lessens the right of those individuals to know that they were under suspicion. In the event that they were wrongly suspected or the suspicion was based on erroneous information, then the right of access or notification would result in them being able to pursue that through whatever appropriate avenues exist, whether that be the pricing commission or the ombudsman.

Ms MARINO: Possibly, given that they were not part of an ongoing investigation.

Mr HAWKE: I want to turn to your comments on carriers. You have not really spent a lot of time on carriers. Why might that be? It says here that you regard it as essential that the bill provides an explicit requirement on carriers to store data subject to preservation notices in a secure manner. But have you considered what happens to the data post that point? There is no requirement under the current legislation. It does not specify what should happen with data that has been stored under one of these orders.

Mr Waters: Thank you for drawing our attention to that. That is probably an area that we could have spent more time on, but in our haste we did not. We would certainly like to see a comprehensive regime in the bill for what happens to preserved data. The other point is that that highlights the need for a contextual discussion about the government's intentions in relation to data retention.

Mr HAWKE: Agencies are required to destroy it under the amendments.

Mr Waters: Under the Privacy Principles.

Mr HAWKE: Yes.

Mr Waters: The Privacy Principles already require them not to keep that information for longer.

Mr HAWKE: But carriers are not. You would agree generally with the principle. With agencies, at least there is oversight and scrutiny. There is the ability for people to look at that. But with carriers there is very little recourse and that makes it difficult for people to understand what is happening with their data.

Mr Waters: That is true. They are not necessarily data users under the Privacy Act. Thank you for pointing that out. We would certainly be looking for specific—

Mr HAWKE: Yes. I just wanted to understand your view on that point in particular. I had made a guess, and your comments confirm that. In relation to this issue of foreign powers, do you agree with the general principles of the cybercrime convention, such as the serious categories of crime and sharing information in that regard?

Mr Waters: Yes, subject to appropriate safeguards on how that information will then be used. We would take the view that there are some countries that are probably so rogue, if you like, that you simply could not trust the assurances that you were given by them.

Mr HAWKE: Sure. I want to follow this line of inquiry for a minute. In relation to this issue, essentially what you are raising there is the operation of criminal law and civil law in different countries. You suggested the example of copyright, which would be a civil matter here but which could be a criminal matter in other

jurisdictions. This information was provided in some other evidence, but isn't that covered by the dual criminality principle? Isn't that covered under that section?

Mr Waters: It should be, but our understanding—and again we defer to some of the civil liberties submissions for probably a better explanation of this—is that there is not an adequate dual criminality criterion in this bill.

Mr HAWKE: So the view is that that could be bypassed. Do you have an understanding of why that is? We had strong evidence that said that would not happen, so I would love to get a better understanding of your view about that.

Dr Clarke: Did you have strong evidence or strong assertions about that?

Mr HAWKE: Strong assertions.

Dr Clarke: Yes. We would like to see the evidence, and we have not done so. We therefore are very dubious about this.

Mr HAWKE: But what is the basis of your contention that that could be the case? Do you think it is subject to legal test? That is what I am trying to get a feel for. You have raised that point, and it could be a very valid point—I do not know. I just want to know what the basis of your reasoning is there. It has been put to us that if the Australian authority does not have a similar offence here in Australia then there will not be warrants or other notices issued.

Dr Clarke: We are stalling for time on this one because the third member of the primary drafting group, who is at the University of Queensland and could not get down here today, is the one who drafted that section.

Mr HAWKE: You mentioned that. If you have to take it on notice, that is fine, but I would appreciate that follow up in terms of the intellectual property that we mentioned either. If that is what the issue is related to, that would be interesting.

Mr Waters: It is much broader than that.

Mr HAWKE: I agree. I am asking for a bit more. But if you need to go to a particular person, I am happy to get that later.

Mr Waters: We are happy to take that on notice.

Mr HAWKE: We will do it that way, then; that is fine by me. I would appreciate that, because that could be quite significant. Finally, you mentioned one other area that I wanted to ask a question on. In terms of the scope of stored communications, you have said that it recognises the privacy sensitivities. Let us look at the delineation in the current amendment between traffic data and content. You have said that the existing acts have good provisions but these amendments jeopardise that. I specifically want to understand that. Is that because of sloppy drafting in your view? Are you saying there could be some tightening in relation to the language in the bill? You made the claim there that this would lead to agencies being able to access different data than what they can now. I think you said something about language. I want to really understand this.

Mr Waters: I think it is a combination of a substantive problem and some sloppy drafting.

Mr HAWKE: What is the substantive problem?

Mr Waters: My understanding is that this will allow preservation notices and subsequent access requests in relation to stored communications that might not be subject to a warrant.

Mr HAWKE: Under the telecommunications interception act?

Mr Waters: That is right.

Mr HAWKE: Do you think there is a weaker threshold?

Mr Waters: We may be wrong on that but it is too obscurely presented to be sure. That I think needs to be clarified. The sloppy drafting is basically in some of the references, particularly in the explanatory memorandum, to stored communications when our understanding is that it actually means both stored communications and traffic data.

Mr HAWKE: So your interpretation of it is that it is both but it says just one type.

Dr Clarke: It uses an undefined term. The key sentence, as we have got it, is:

As currently drafted, the Bill does not specifically differentiate between—

things that have been previously differentiated importantly in the law—

traffic and content data and instead merely refers to "stored communications" which is not defined.

Thereby anything might happen because the courts would have to decide.

Mr HAWKE: I have got that. I have not seen the term 'traffic data' either in this draft, but your point is that there is this distinction and it is not clear.

Mr Waters: Yes, it is not clear and it is not consistent with the existing regime.

Mr HAWKE: Do you have a view about the length of time in relation to the operation of these warrants and orders—90 days and 29 days? Does your organisation have a view?

Mr Waters: To some extent that is always going to be arbitrary. Without giving it any more thought, it does not strike me as unreasonable.

Dr Clarke: We have not had time to consider details like that. We have been trying to probe what the major issues are.

Mr HAWKE: I appreciate that.

Dr Clarke: We are going to be silent on that one at the moment, I am sorry.

Mr HAWKE: I am just checking through some of the different bits and pieces we have heard from other people on. You used a phrase that we also heard this morning. I think you referred specifically to the operation of backdoor mechanisms.

Mr Waters: The concerned there is that if the definition of telecommunication service actually applies to a service operated by, say, Telstra to a range of customers then that potentially allows for the issue of a preservation notice to Telstra saying, 'Please preserve the information of all the customers to BigPond,' for instance, whereas we understand the existing interception and access regime requires specification of a named individual or a named number, if you like.

Mr HAWKE: This is the weaker threshold argument.

Mr Waters: That is right. Because 'telecommunication service' has not been defined separately, you are left wondering whether it actually means the same as it does under the existing regime.

Mr HAWKE: So this could be dealt with by greater definition of what is required for a notice?

Mr Waters: Yes.

Mr HAWKE: That is good. Thank you.

CHAIR: I would like to go back to people being told that they have been investigated. Are there any jurisdictions in which an individual is notified once investigations are complete that he or she was subject to a warrant order or authorisation?

Mr Waters: The one we are specifically aware of is the United States. In most cases people who are subject to wire-taps—the equivalent of interception warrants—are notified once they are no longer under suspicion or investigation. There may be others.

CHAIR: Do you know of any European privacy directive or human rights instruments that require that sort of notification?

Mr Waters: I will have to take that on notice, Senator.

CHAIR: If you could, that would help. A quick question from Ms Marino. We have a teleconference scheduled.

Ms MARINO: You are very strong about secondary use. How would you see that being written into the legislation and basically how would that be enforced beyond the legislation, in your view?

Mr Waters: I think there have to have a much stronger assurances given by the overseas agencies and much stronger monitoring, so a role for an independent monitor to follow up and see whether there is any evidence that those assurances have been breached or to investigate allegations that they have been. There should also be provisions that allow Australian agencies to basically discontinue cooperation with any overseas agencies which breach those assurances.

CHAIR: Dr Clarke and Mr Waters, thank you for attending the hearing and giving evidence today. Your participation has been a valuable contribution to the inquiry. The secretariat will contact you if the committee has any further questions.

Mr Waters: Thank you very much. We will let you have those answers to questions on notice.

CHAIR: That would be wonderful. Thank you. I might tell you that the submissions are now on the website.

CONNOLLY, Mr Chris, Research Associate, Cyberspace Law and Policy Centre, University of New South Wales

VAILE, Mr David, Executive Director, Cyberspace Law and Policy Centre, University of New South Wales

[11:47]

Evidence was taken via teleconference—

CHAIR: Welcome.

Mr Vaile: We have agreed that to keep things simple. Chris Connolly will provide the main initial commentary because of his extensive background, particularly in the Asian region. We had hoped that the author of our submission, Alana Maurushat, would be able to speak directly to our submission but she is not available today, so we are trying to assist the committee there.

CHAIR: Thank you for that. Although the committee does not require you to speak under oath, you should understand that these hearings are formal proceedings of the Commonwealth parliament and giving false or misleading evidence is a serious matter and may be regarded as contempt of parliament. I remind you that the hearing is public and is being Hansard recorded. The hearing is also being broadcast live. I ask you now to make a short introductory statement and the committee will then proceed to questions.

Mr Connolly: Thank you. We welcome the opportunity to present to the committee today and to complement the written submission that was submitted on our behalf. We would like to start by saying that the centre has a strong belief in the harmonisation of cybercrime laws around the region and around the globe, and we therefore support the intent of the bill, which is to accede to the Convention on Cybercrime. We see many benefits from that accession. However, we do have some concerns—and we share these concerns with other interested parties—that the bill may go further than is necessary to implement the convention. We would like the opportunity to present a few of those key points now.

The first concern—and it is a major one—is that the bill, as we read it, does not appear to directly address the issue of dual criminality. For example, mutual assistance can be provided to other countries—preservation notices can be exchanged, for example—without there being a clear and unambiguous test of dual criminality; that is, any criminal offence that is the subject of mutual assistance should be an offence both in Australia and in the target country. Australia has a more limited set of cybercrimes than exist in many other countries. A good example is that sedition is no longer a criminal offence in Australia, yet it remains a criminal offence in many other countries, including some countries in the region. That is a core part of our test of whether or not the bill is acceptable: whether or not there is a clear and unambiguous requirement for dual criminality. The convention allows countries to make reservations related to dual criminality requirements, so it is already anticipated that countries would do that.

The second concern is just a list of concerns around preservation of data notices. It is our belief that the standard should not be set too low for when data should be preserved. For example, the bill has established that data can be preserved or a notice can be presented for data preservation where an offence has a maximum penalty of only three years. We believe that alternatives should be considered. One alternative would be to provide a specific list of cybercrime offences, and the preservation notices should only relate to that specific list. A second option would be to say that preservation notices should be reserved only for offences where the penalty in Australia was a three-year penalty and above. We are quite aware of a number of other jurisdictions, especially in our local region, which have very high sentences for offences which would be considered quite minor in Australia. We believe the test should be the Australian penalty, not the penalty overseas.

Further, we would recommend that the type of oversight and public reporting which currently applies to warrants and interception notices et cetera should also be applied to all preservation notices by all agencies. We do not want to see a sort of separate lower standard of oversight and reporting implemented for data preservation notices, because we believe that they will be an important part of law enforcement in the future. They are susceptible to abuse and we would like there to be as much transparency and openness around their use as possible.

Finally, where data is preserved as the result of a preservation notice and mutual assistance, we believe that the bill should include a requirement that appropriate security standards are applied to that data and that, when the 90-day period—or whichever period is appropriate—expires, the data should be destroyed in accordance with

appropriate security standards, so that the data has another layer of protection while it is in that status of being preserved. We were also a little bit surprised to see that one of the core conditions in the convention is not included in the bill, specifically in section 107J of the bill—that is, the preservation of data should only occur where there is a danger that the data would be modified or lost. Those words are in the convention but they are not anywhere in the bill. They really should be the opening criteria for all data preservation notices and we think they should be explicitly set out in the bill.

I just wanted to mention one or two other points unrelated to the preservation of data. The first is that we believe it is important that the Criminal Code is amended to include the same definition of a device as appears in the convention. Our reason for that is we are concerned that botnets, which are an important part of attacks which occur in cybercrime, are networks rather than individual devices, and they are information rather than individual devices as defined in the Criminal Code. In fact, they are covered by the Convention on Cybercrime, which has a broader definition because it includes networks and information rather than just physical devices. That would be an improvement.

We also believe that the bill, as we read it, is unclear in its definition of stored communications in that the convention very clearly, for each clause relating to data retention, says whether or not it is referring to traffic data or content—that is, the content of the communication. The bill, however, uses the broader generic term of 'stored data'. We are not comfortable with that. We think that because the convention always distinguishes between traffic data and content that the same distinction should follow right through the bill in implementing the convention in Australia.

Finally, I believe you have already heard some submissions on privacy earlier today, but we share a concern around section 180F of the bill. This is where the organisation considering a request for assistance is asked to 'have regard to privacy concerns' but that is the full extent of the test. Having regard to privacy concerns is a weak test in a law enforcement environment. We would prefer to see that test include a specific requirement to weigh up privacy against the other interests of the investigation and to make a firm conclusion based on that test, rather than simply having to tick a box and say, 'Yes, we have had regard to privacy and now we are going to move on.'

I hope I have conveyed some of the main points from our submission. There are a few other points in there and we encourage you to read it. My colleague David and I are very happy to take additional questions.

CHAIR: Thank you. Mr Vaile, do you want to make an opening statement as well?

Mr Vaile: Yes, I might just touch on a couple of other points. In relation to the protection of personal information security and privacy, I think it is important to acknowledge that, for the purposes of pursuing the most serious forms of cybercrime, we are envisaging, through accession and implementation of the Council of Europe's convention, some diminution and some attacks on the integrity of communications data and personal information security. As part of trying to work out whether the balance has been achieved—because privacy, security, human rights and law enforcement all require a balancing operation—it is worthwhile considering the context and framework that this bill would be introduced into. The first point is in relation to the expansion of the powers of what used to be called the Privacy Commissioner's office, which is now embodied in the office of the Australian Information Commissioner as a privacy function. This bill should not continue without additional attention to fixing any deficits within the jurisdiction of the Privacy Commissioner's office—and I will use that old term for the moment. To provide the safeguards for Australian internet users in particular, questions about enforceability of decisions and the power to impose fines on ISPs and others where there are unwarranted, unjustified and unauthorised breaches of an internet user's privacy should be addressed as part of the package. Without that and a number of other protections which I will touch on in a second, even a revised version of the bill would not be suitable.

The second point, more generally, is that as a result of research from a number of people in the field and the Australian Law Reform Commission's report 108 there is a range of deficiencies in existing privacy law that would not be fixed by that minor extension of jurisdiction that I have just mentioned. The widely accepted and increasingly topical solution to that problem is some form of cause of action. Some people have called it a tort. It does not necessarily need to be a tort, but it does need to be a legally enforceable right to the protection of privacy on the basis of individuals that does not require as the only solution a complaint to the Privacy Commissioner's office. We see that this bill should not go ahead without, as part of the package of its passing, the introduction of much more robust statutory protection for privacy.

The other minor point is that small internet service providers at the moment are exempt due to turnover thresholds from obligations under the Privacy Act, to the extent that the Privacy Act is going to be useful as a protection here. If those ISPs are to be brought within the ambit of this bill then the scope of the National Privacy

Principles, however they are described, must be included within that. It is not appropriate that they be included under this bill without also being under the protection of the Privacy Principles.

A couple of other comments we would like to make involve the transparency of the regime. I understand from comments I heard from the previous speakers that there was a reference to greater transparency and obligations in the US in particular after the orders foreshadowed here have completed. That is a useful example of a more general question that should be addressed in reviewing and reconsidering this bill. The general principle is a question about independent oversight and transparency of the operation of these highly intrusive measures—the preservation notices. There is also the capacity for wide discretions about government agencies being able to request them under ministerial authorisation.

Both the general introduction of these more intrusive measures and the operation of those wide discretions can only be considered, in our view, if there is much greater transparency and in fact a commitment as part of this package to transparency, rather than what we have sometimes seen in the past which has been an idea that if you are including greater measures of surveillance and intrusiveness then as part of that package you also make it more difficult to talk about them, more difficult to oversee them and more difficult to publicise aspects of their operation. We see that the necessary balance, if something like this bill were to be considered, would include, in principle, a much greater commitment to transparency and increased measures to implement that sort of approach.

I would like to mention some possibly more minor points. One is in relation to research and the capacity to conduct cybercrime and malware and botnet research that is legitimately done with appropriate safeguards and transparency itself without having the researchers having to worry about falling foul of offences that were not really intended to catch them. So it is very important that security research exemptions or some similar mechanism to support research, particularly in both technical and regulatory aspects of this area, can occur without that sort of worry on the part of the researcher.

The final point is that I wanted to refer to a gap in the coverage of existing cybercrime laws that might warrant some consideration in the context of this bill, and that is the use of spyware, adware and a variety of other forms of not explicitly authorised technology to insert software or software components or other sorts of tracking technology without the effective awareness and consent of the user. As part of this bill, in order for that operation to become properly subject to the criminal law, where it turns out to have been done in appropriately malicious circumstances, if you like, the installation of such software or software components on user computers over the network, particularly over the internet in Australia, should become expressly illegal. Given that there are some opportunities in this bill to fix up minor jurisdictional problems, we see that this is an opportunity here to remedy that defect. That is the end of my opening comments.

CHAIR: Thank you, Mr Vaile, for that quite in-depth introduction. It is very difficult working by teleconference, where we cannot see each other, but we do really appreciate it. Mr Hawke has some questions for you.

Mr HAWKE: Can I ask a quick technical question: how long has your centre been operational?

Mr Vaile: Since around 2001, so that is about 10 years.

Mr HAWKE: Thank you; that is good to know. I want to address a couple of things in your submission. You have made a recommendation which I think is a little bit outside the scope of the legislation. You talk about the fines for internet service providers. Do you have any body of evidence that suggests that internet service providers are breaching people's privacy on such a basis that we would need to have a fines regime?

Mr Connolly: I think the Law Reform Commission's review of privacy did receive quite a lot of evidence around the lack of privacy enforcement in Australia and obviously has made recommendations about strengthening the Privacy Commissioner's powers. What we have noted as the centre is that, in the decade since the privacy provisions were extended to the private sector, only one actual determination has been made by the Privacy Commissioner against a private sector operator, and that was the result of a class action, a representative action, by consumers against a tenancy information service. Ten years is a long period without any actual enforcement action. No organisation has been named as being in breach of the Privacy Act as a result of a complaint. This compares unfavourably with sectors such as the regulation of telecommunications, financial services, the activities of regulators like ASIC and the ACMA where organisations are named fairly regularly as being in breach of legislation such as the Spam Act, the Do Not Call Register Act, the Corporations Act et cetera. We believe there is a strong body of evidence and a good 10 years history showing that the conciliation approach, which is the approach of the Privacy Commissioner, remains unusual in the regulatory sphere and really does not provide any motivation to comply with privacy laws.

Mr HAWKE: But certainly in relation to the scope of this legislation and you are advocating that data retained by carriers for 90 days—under the preservation, retention and destruction of data clause in 1.6—be required to be destroyed after that period of time.

Mr Vaile: It would certainly be our expectation that the data would be destroyed on expiry of the notice. I think 90 days is the default period. We would not expect notices to always lead to the preservation of data for the full 90 days. Obviously our concern is that, if that is simply left to the current privacy arrangements, the worst that a service provider could expect is a private rap on the knuckles for retaining the data for a longer period and for even other abuses of privacy.

Mr HAWKE: That is an important point. So you are saying that it is not necessary for it even to go the full length of the 90-day period?

Mr Vaile: Our understanding is that the 90 days is a default but that the notice could specify that in fact you are requested to preserve the data for a shorter period—for 10 days, for example—and it is only if the notice does not include a shorter period that the 90 days would act as the default.

Mr HAWKE: On the issue of dual criminality, I think you have expressed it with greater clarity than anyone this morning. Your view is that it is possible for that to be circumvented under this proposed legislation, that you could have a civil offence in Australia which is a criminal offence in a foreign jurisdiction being activated under this current draft?

Mr Vaile: Absolutely. We are unclear whether it is the intention of the drafters or whether it is a drafting error. Normally what you would expect to see in a bill of this type implementing a convention is a specific decision by the legislature to act on the recommendation in the convention that countries can choose to impose a dual criminality requirement for all of the subsequent cooperation arrangements such as data preservation notices, mutual assistance et cetera. There is no dual criminality requirement in the bill. There is nothing set out and a reading of the bill states that a preservation notice might be considered compliant simply because, for example, an offence in a foreign country has a maximum penalty of three years or above with there being no other requirement that that same offence would be an offence in Australia.

In cybercrime you have to understand there are very different approaches in different countries. Some countries have made certain types of speech the subject of criminal offences and Australia has specifically, following a national campaign and recommendations of the Australian Law Reform Commission, removed criminality from those exact types of speech. You would have seen that in the Law Reform Commission's report on sedition laws. Some countries have made certain types of speech the subject of criminal offences and Australia has specifically, following a national campaign and recommendations of the Australian Law Reform Commission, removed criminality from those exact types of speech. You would have seen that in the Law Reform Commission's report on sedition laws. So I think it is really important that we ensure that dual criminality is set out explicitly in this bill.

Mr HAWKE: I appreciate that. Can I just cut you off, because I am taking up a lot of time with these questions. I have a couple of final questions and it would be good to have brief answers. On that issue, you are saying that using the Australian law as the standard would be one way of solving the issue of the three-year penalty minimum. That is not currently in the draft bill, is it?

Mr Connolly: No. At the moment the three years refers to the foreign penalty. Of course, it would be easy enough, because cybercrimes are becoming so harmonised, to assess what the equivalent offence in Australia is.

Mr HAWKE: Would that still create obligation under the convention? Is that going to fill the requirements? That is the thing we would have to be certain of.

Mr Connolly: Absolutely, and our understanding was that it would be completely normal practice under the convention that signatories to the convention would set their standard for when an offence was a serious foreign offence and this would not be an opportunity to remove or reduce our sovereignty in any way. The standards for data being exchanged would be based on Australia's understanding of what a serious foreign offence is.

Mr HAWKE: Thank you for that. I appreciate it very much.

Ms MARINO: Thank you, gentlemen. The bill basically does not restrict the foreign countries that we could provide assistance to. Do you see any issue or any inherent difficulty with that unrestricted approach? Some submitters have expressed concern about a country like China. Do you have a view?

Mr Connolly: Our view is set out in a written submission and that is that, unlike some other submitters, we accept that a broader list of foreign countries could be considered for cooperation than the narrower list of just those countries that have signed the convention. As you are probably aware, the convention is contentious in a lot

of countries because of the intellectual property provisions, not because of the cybercrime provisions, but Australia still has a good level of cooperation with those countries on cybercrime. Obviously, if we restricted it just to the very narrow group of countries who signed the convention, that would limit opportunities for mutual assistance and cooperation.

However, having said that, we are a bit concerned that the government's approach to which countries we would provide assistance to and in what circumstances is becoming splintered—it is becoming spread out amongst the number of different pieces of legislation and different government policies. It would be useful to see it all included in one piece of legislation. For example, Australia does not cooperate in circumstances where a person might face the death penalty, but that is only set out in some guidance to the Australian Federal Police; it is not set out in legislation—it is not, for example, included in the bill before you today.

Another example is that the convention says, 'You don't have to cooperate if you suspect a request is politically motivated.' That is in the convention, but equally that could appear in the bill. So I think it would be good if, instead of restricting the number of countries to just those countries that have signed the convention, we set out a better set of criteria for all of the countries that we would consider cooperating with.

Mr Vaile: May I respond to that question?

Ms MARINO: Certainly.

Mr Vaile: This is a partial response to an earlier question as well. The general context of the bill is one where the role of the ISP appears to be changing from a simple contractual agent of the customer to a surveillance role on behalf of other parties, including local authorities but potentially also foreign litigants, for other purposes. One of the contexts of our raising concerns here about protecting Australia's sovereignty and the sovereignty of legal protections for Australian citizens is that if that sort of process is occurring, if the ISPs are being recruited to have in a sense a conflict of interest between their two different roles, it is extremely important to include very strong protections, very explicit acknowledgements of the limitations, reservations and other qualifications we have about the operation of the convention. In particular, where we are going down that path—and it is not a path that I think should occur without comment—to the extent that there are protections and balances within the convention itself, they should be explicitly used.

The explicit acknowledgement of dual criminality is important there. Also, the other opportunities for introducing much more transparent and visible operation of these sorts of approaches should be seen as part of that package. It is not merely a matter of encouraging cooperation with foreign law enforcement agencies, which is something we support in appropriate circumstances; also, we should not take that as an open-ended licence for scope creep in relation to the role of ISPs and in relation to the use of these sorts of powers and notices.

CHAIR: I thank you for participating in the hearing today and giving evidence. It is obviously a bit more difficult to do that by teleconference than face to face, so we thank you for that. Your participation has been very valuable. You have made a valuable contribution to the inquiry. The secretariat will contact you if the committee has any further questions. Once again, thank you for your participation today.

FROELICH, Mr Peter Anthony, Principal Domain Expert, Telstra Operations, Telstra

SHAW, Mr James, Director, Government Relations, Telstra

[12:23]

CHAIR: Welcome. Although the committee does not require you to speak under oath, you should understand that these hearings are formal proceedings of the Commonwealth parliament. Giving false or misleading evidence is a serious matter and may be regarded as contempt of parliament. I remind you that the hearing is public, it is being recorded by Hansard and it is also being broadcast live. I invite you to make a short opening statement and the committee will then proceed to questions.

Mr Shaw: Telstra thanks the committee for the opportunity to appear today and discuss the Cybercrime Legislation Amendment Bill. As stated in our submission to the committee, Telstra is generally supportive of the proposed amendments to the legislation to ensure that Australia is compliant with the treaty conventions of the European Convention on Cybercrime. We believe that these proposed amendments will assist in improving the processes and procedures used by carriers and carriage service providers to provide law enforcement agencies the information they require to deal with cybercrime and improve cybersafety—

CHAIR: Mr Shaw, we have a camera in the room. Are you happy to be filmed and have photos taken? Sorry, I should have checked that with you before.

Mr Shaw: That is fine. We love democracy! There is one issue on which Telstra has made some representations in respect of the legislation, and that is around the implementation time frame for the new arrangements. The activities required to comply with these new arrangements are likely to require carriers and carriage service providers to divert a significant amount of time and financial resources and they are likely to involve significant amendments to our network and IT systems, which in a company as complex as ours are not straightforward. We suspect they will also involve a reconsideration of capital programs and business planning programs within the business.

Mindful that we want to ensure that new systems and processes put in place to support the new arrangements are robust and secure and have no unintended consequences for either ourselves or our customers, we believe that changes should be made to the implementation arrangements proposed in the bill. The time periods that are requested in our submission, we believe, would be used to determine the extent to which our existing networks and IT systems will require modification or even replacement to ensure compliance with the long preservation periods envisaged.

Time is required to undertake the detailed feasibility and impact studies, including the engagement of vendors to design and cost the modifications to existing networks and IT systems, to investigate the new logical and physical security and privacy processes and procedures needed to protect the preserved information from unauthorised access and to task additional resources into the programs of work to support those outcomes.

Time is also needed to design, build and integrate the new systems and network upgrades to preserve our computer and telecommunications data to make sure that the data that the law enforcement agencies have requested is safe and secure. Time is also required to develop, deploy and test new formatting and hand-over standards with the lead agencies that will enable the secure delivery of preserved data to law enforcement agencies.

To facilitate the introduction of these new arrangements and to allow carriers and carriage service providers to undertake the technical feasibility studies outlined above, Telstra suggests there be an implementation study period of 90 days following the royal assent to the bill, to enable the carriers and carriage service providers to undertake the necessary feasibility and impact studies on our networks and that there should then be an exemption process for carriers and carriage service providers of up to 18 months following that implementation study period, to enable carriers and carriage service providers to physically design, build, integrate and test the new systems and network upgrades to ensure that the data the law enforcement agencies have requested can be delivered in a secure and safe method according to the lead agency standards.

Finally, although we did not raise the issue of cost recovery in our submission, Telstra also believe that the additional obligations to preserve data are beyond Telstra's business needs and should be subject to further discussions with the government, as the proposed amendments, we believe, will place a significant resource burden on carriers and carriage service providers in the form of cost and manpower. We will be pursuing those issues with the government outside of this forum. That concludes the statement. Thank you.

CHAIR: Thank you, Mr Shaw. Mr Froelich, do you have anything to add?

Mr Froelich: No.

CHAIR: You suggest in your submission that there is no standardised way to respond to law enforcement requests currently in existence. What is the current practice of Telstra for preserving data in response to a stored communication warrant?

Mr Froelich: Where those tools and facilities are available, we operate under the terms of the current Telecommunications Act to preserve the data at a best effort attempt. In terms of how we actually transfer that information to requesting agencies, it is generally by paper response, which is printouts of stored requests and so forth.

CHAIR: At what point do the employees of a carrier start to collect and preserve the data? Does this happen before the stored communication warrant is issued?

Mr Froelich: I believe that, when we get a preservation request from a law enforcement agency, we act immediately on that request, with the formal notification to follow that.

CHAIR: We have heard in other submissions that quite often information is destroyed within a 24-hour or 48-hour period anyway. Is that the same with Telstra in general?

Mr Shaw: We have varying periods of retention for various types of data.

CHAIR: Are you able to expand on that for us?

Mr Froelich: Where the business need does not require us to keep that information, we would make every effort to destroy that as soon as the business need dissipates. That business need is around network access, billing, network surety—those sorts of things. If there is no business need, there is no rationale for us to keep the data, so therefore we destroy it.

CHAIR: And so if there is a warrant put in place, what is done with the data once it has been collected and disclosed to the appropriate agency?

Mr Froelich: Could I have that another way?

CHAIR: A warrant has been put in place, the information has been collected and it has been transferred to the agency. What then happens to it at the Telstra end? Do you destroy it? Do you keep it?

Mr Froelich: After we have been through that process, I believe we destroy it. But I would have to take that question on notice to give you a more detailed response if required.

CHAIR: If you could, and within what time frame that might happen too. That would be useful. Do you expect there to be a significant increase in the assistance to the agencies due to these amendments?

Mr Shaw: We have not scoped out the exact impact on our network as a consequence of these amendments, Chair. I would be guessing if I was to give you an answer. One suggests that there would be an increase simply by the nature of the amendments and the ability of agencies to collect information, and simply by the greater instance of use of telecommunications networks for people to use to communicate and converse. The answer would be 'yes', but to what extent we would be guessing.

CHAIR: So obviously you would see benefits in having a standardised way of handling the requests and collecting the data and delivering that data to the agencies—is that core of your submission?

Mr Shaw: Absolutely yes. We see a lot of benefit for us from the business end, in our capacity to respond to these warrants in an organised way and have business processes in place that mean we can hand across this information in a secure form. We also think that having standards in place and systems within our business can ensure that we have greater capacity to ensure the security of that information.

Mr HAWKE: I want to stay on the issue of cost recovery for a minute. It is already the case under the law that you have to provide assistance to law agencies, and you recover your costs—

Mr Shaw: We recover some of our costs.

Mr HAWKE: at a not-for-profit basis. There is a definition in the current standard. I am not understanding this clearly: in relation to the provisions in this bill and what will happen, you are envisaging an increase in requests from law agencies?

Mr Shaw: It is not necessarily that we envisage an increase, but we know that we are going to have to change our systems and incur costs simply to comply with the legislation.

Mr HAWKE: The new legal requirements.

Mr Shaw: Yes.

Mr HAWKE: Okay. In relation to that, I am concerned about what you said about 18 months. The criminal law is one of the primary functions of government, and this is to deal with categories of crime that are quite serious, so 18 months seems to me to be a very odd period of time for you to be seeking for compliance. It is not as if this is not compliance with the law and criminal law in particular areas; it is a fundamental responsibility of all of us, and these agencies are pursuing these matters on behalf of all of us to track down serious criminals and do the right thing by all of us. That is why we have government. I am all in favour of business in terms of regulatory burdens imposed by government that are unnecessary, but we are talking about criminal law. I would ask: why do you need 18 months to comply reasonably with what is a very reasonable request from government?

Mr Shaw: It is a fair observation. The 18 months is an exemption period for compliance. It may be that we do not need the full 18 months in some instances where we need to change our network and our IT systems. But changing IT systems and the network systems in a telecommunications business is not a straightforward proposition. Our IT change program runs out two years in advance. So if we schedule even a small change in our billing arrangements, a decision is not made one day in the business and then the IT people make those changes the week after. These things are many, many months out because we have to ensure that any changes made in one part of the network or the IT system do not have unintended consequences elsewhere, do not deliver corrupt data, do not divulge data that should not be divulged and the like. So the period of 18 months, we think, is a reasonable period to enable us to have up to—we do not say that we necessarily have it in every instance—to ensure that the systems that are built are robust, they operate in conjunction with our existing business systems, they deliver data that the law enforcement agencies can rely upon and that our customers can be certain is being kept and transferred securely. Over and above that, we envisage that because there are costs we actually have to go back into our capital management program and find the money that will be necessary to build all of this, and that is not straightforward process. Equally if we have to go to our vendors and commission further work on our network to get this done, we have got procurement process and other things to go through. So the nature of business which is so heavily reliant on ICT and which is as capital intensive as ours says that 28 days, we cannot guarantee compliance in that period of time. We simply propose a period of 90 days in which we can scope out the extent of those changes and have some certainty about what we can and cannot do and then work with the agencies around an 18-month maximum window for implementation keeping them informed on the way through, and of course best endeavours all the way through there to deliver any information they may need to assist them with their law enforcement activities.

Mr HAWKE: That makes more sense. I understand your thinking in relation to that. So you are suggesting that the 28-day period is not sufficient at the moment for you to provide the data in a way that is legally acceptable.

Mr Shaw: We cannot be certain, given the current time frames in the bill, that we can be compliant in those time periods. And we certainly do want to be compliant.

Mr HAWKE: Absolutely. I suggest that is not negotiable. In relation to this, you are a large corporation but that can often be more problematic for bigger organisations because you have got more customers and more diversity. What you think about your industry: do you think they are going to have a similar view to yours about this?

Mr Shaw: I can point to the fact that the Australian Mobile Telecommunications Association and the Communications Alliance, which are two industry bodies, in earlier parts of the consultation around this legislation with the Attorney-General's Department put in submissions which recommended similar periods and similar arrangements as are put in our submission to this committee.

Mr HAWKE: Have you had any other opportunities to communicate ways you could assist law agencies meaningfully? Do you have a better suggestion on the way the law could be framed? This is a very important area of law and we are dealing with the international obligation we are trying to meet and about criminal activity. I have a great sympathy for law enforcement agencies in what they are trying to do and indeed assisting them as much as possible to get the information they need, and so do members of this committee. Do you have any practical suggestions about the framing of the law that could assist us?

Mr Shaw: We have been in discussions with the Attorney-General's Department and the various agencies and law enforcement agencies through the process leading up to this bill. We also have regular ongoing dialogue with them around a whole range of policy and operational issues in this space. So we think we have very good lines of communication in that area of government to put our point of view. As I said in my opening statement, we are generally happy with the provisions of the bill; it is this one issue around implementation on which we are making representations.

Mr HAWKE: In relation to the destruction of stored information, you are going to be returning to us with that question.

Mr Shaw: Correct.

Mr HAWKE: That would be fantastic.

Ms MARINO: In relation to the issue of the security of information that is collected, one of your team members will be collating this information for the agency that is requiring it. In relation to the security of that and access to it, how are the confidentiality issues dealt with?

Mr Froelich: In terms of being custodians of our customers' privacy, that is obviously mission-critical for us in terms of maintaining that obligation and this act in terms of increasing the preservation of that data, increasing the number of obligations or disclosures we may have to make. That is why Mr Shaw was referencing the need for greater build. In terms of the framework of the act, we would hope for more guidance on how the mechanics of that should work in terms of working into law enforcement. Our expectation is that we should arrange for secure access to our systems, physical and logical security around how we actually retain that data, and the costs involved with that are obviously some of the things we have alluded to. In terms of how we actually arrange that interface to law enforcement, we would like to see more electronically signed documentation interfaces to law enforcement to actually manage that data in a more secure and resilient way. We would like to see an embrace of international standards in terms of how carriers and carriage service providers would work into agencies to manage that security and privacy of customers' data. So it is a fairly sensitive area for Telstra.

Ms MARINO: Extremely sensitive for any ISP, I would think. On international standards, which particular international standards are you referring to? Do you think that any of the factors that you have just mentioned need to be reflected within the legislation?

Mr Froelich: Potentially that can be handled outside the legislation, as Mr Shaw suggested. We are happy to consult with the departments outside of the legislation in terms of the framework of the implementation. But it would be beneficial to have some reference to internationally agreed mechanisms for interface, and standardisation bodies such as the European Telecommunications Standards Institute publish these types of interfaces already and they are in fact in use in European marketplaces. Access to those international standards would reduce bespoke development in Australia, which is something that we definitely want to avoid. We do not want to develop Australia-centric solutions to these sorts of issues.

Ms MARINO: How do you normally recover your costs on any request by an agency now? How do you cover that off within your organisation? How do you currently recover those costs?

Mr Froelich: There is a regime within Telstra's corporate security and investigations team to recover costs on a per request basis. Those costs are managed by that time. In terms of their billing cycles and how they actually work with agencies, I am not totally familiar with that, sorry.

Ms MARINO: But historically that has been sufficient to cover the costs of what you have been required to do?

Mr Shaw: It has been sufficient to recover that which we are entitled to recover. We bear some of the costs of developing systems and those costs are not recovered.

Ms MARINO: That is more the intent of the question.

Mr Shaw: We recover the transaction costs of the request, but the build capability is something that we bear as a cost to our business—as do other carriers and carriage service providers.

Ms MARINO: And that is what you are referring to over the 18-month period: the build cost as well as the cost of providing the information if and when requested.

Mr Shaw: Correct.

CHAIR: Can you tell me why this legislation, which will lead to requests to carry out a legal duty to preserve duty, is such a significant reform for carriers and carriage service providers? I can see why it impact on smaller providers, but I am not quite sure why it would have an impact on such a big provider as Telstra—bearing in mind that there are obviously going to be more requests, although you cannot say how many more. But you can say that you think that you need 18 months to come into line. Surely you have known about this for a while. I am just a bit confused. I cannot quite get clear in my head why you think that you need so much time.

Mr Shaw: First of all, we have been aware of the proposals around session two of the convention since the government announced that it was going down that track. However, that in itself is not sufficient for us to be able to get capital within our business to start building any of these systems. We cannot go to our management and ask for that funding until we have a legal obligation to build these networks. As a bigger company, the point that

flows from that is that we have more customers and therefore we will have to preserve more data. That comes at a cost. The fact that we have to preserve more data and transfer that data to the agencies leads us to want us to try and do that in the most efficient way but also in the most robust and secure way. The need to potentially keep a large amount of data preserved for a period of time means that we have to have a whole new business process around keeping that data in a place that is accessible but secure from unauthorised access. It is not a straightforward task. Bear in mind that at the same time as we are looking at implementing the necessary tools to meet the obligations that may arise under this legislation we—as is the rest of the industry—are making a whole range of systems changes within our business to start to interface with the National Broadband Network, to introduce IPv6 into our network, to introduce mobile location services for E000 into our network and to put emergency alert systems into our network. So there is a whole range of law enforcement, public safety, national security and industry structure issues that we are grappling with in our network at the moment aside from just our day-to-day business of building new products, putting them out to our customers, billing them for those, supporting them, provisioning and whatever else. It is simply the breadth of activity that is going on in our place at the moment, with some fundamental, once-in-a-lifetime changes when you talk about things like IPv6 and NBN, that mean that we have an awful lot happening in our IT and network space.

CHAIR: When you talk about storing more data, are you just talking in regard to that data that has been requested?

Mr Shaw: Correct—only that which we are legally obliged to keep under this legislation or which we have to keep for our own business purposes for the period of time that is necessary.

CHAIR: At this stage you cannot pre-empt how much that might be or anything, though, can you?

Mr Shaw: We know how much data goes across our network and we know what an average user might use, but when it comes down to people of interest that an agency may seek to look at for operational purposes and how much they may generate—or classes of persons or classes of traffic—it is unscoped at this point in time.

Ms MARINO: On behalf of your customers and your clients—you touched on the privacy issue—what would you like to see within the legislation in relation to potential secondary use of the information that is provided?

Mr Shaw: I do not think that is really an issue we have turned our mind to, to be quite honest. Our focus in dealing with this legislation has been around our obligation to preserve and then provide that legislation and how we can do that in the most cost-efficient way, bearing in mind the need for utmost security around the preservation and then transfer of that data.

Ms MARINO: Given the demands on your time in other ways and the interests of your clients being paramount, I would be very interested in your view of how that needs to be reflected to protect their rights within the legislation.

Mr Shaw: So it is around the secondary use of the data.

Ms MARINO: The potential secondary use of any data that you provide.

Mr Shaw: We will take that one on notice.

Ms MARINO: Thank you very much.

CHAIR: Mr Shaw, what percentage of the residential and corporate market in telecommunications and internet services does Telstra represent?

Mr Shaw: It varies depending on the market. I think it is 40 per cent of residential broadband and 40 per cent or the high 30s in mobiles. In the PSTN space I think we are up over 60 per cent or of that order. I can get you some figures.

CHAIR: That would be handy for us if you could. Also, you have storage data for individuals—for me, for example—but do you also have it for businesses or things like that?

Mr Shaw: We do.

CHAIR: Would you store more for those businesses and things?

Mr Shaw: Absolutely. We are servicing the big banks, for instance, so you can imagine what the data retention needs might be in that space. We have a lot of government agencies, and we are putting a lot of effort into providing products in the cloud, as it is now called, where you have virtual arrangements with software as a service and infrastructure as a service.

CHAIR: Just to interrupt, can you explain to me this 'in the cloud' bit. I am not that technical when it comes to that sort of thing. I have heard it a few times. I am not quite clear on what it means.

Mr Froelich: Essentially, if you do not want to own a computer yourself in terms of the raw processing you need to do your day-to-day activities, you can buy computing, storage, services and so forth that sit in someone else's facility. You pay an access fee to use those services as you require them, not to have them dedicated on your desktop or whatever. So you can connect to that and call down your text-editing tool, your editing tool or your mail tool—whatever you need—on a per-usage basis rather than having the dedicated tools—

CHAIR: Rather than having them permanently.

Mr Froelich: with the obligation to maintain, upgrade and have enough knowledge about those systems to keep them running. So you pay someone else to do that part of that work for you rather than having to maintain it all yourself. It is a good concept for the majority of business not to have to retain their own IT departments and comms departments; they can outsource those components to someone that can provide those facilities to them on a daily basis.

CHAIR: So you would retain all that data as well if you are doing that.

Mr Shaw: Correct.

CHAIR: Thank you.

Ms MARINO: I want to ask about the potential for foreign interests looking to access information about targeted clients via their own internal agencies. Do you see any commercial conflict of interest issues or even any potential commercial property rights issues for your clients in the information that you might be required to provide to another agency that is foreign?

Mr Froelich: I guess our expectation is that the local law enforcement agencies would facilitate all that interaction with foreign agencies. We would not necessarily deal with them on a one-on-one basis. We would expect them to filter any requests or information accordingly.

Ms MARINO: And deal with any problems that arise out of that?

Mr Froelich: We would not expect to actually deal with those sorts of issues.

Ms MARINO: Thank you.

CHAIR: Do you have anything else you would like to say?

Mr Froelich: I think we have covered most of the issues.

CHAIR: Thank you for attending the hearing and giving evidence today. Your participation has been a valuable contribution to the inquiry. The secretariat will contact you if the committee has any further questions.

Proceedings suspended from 12:51 to 13:31

CHIDGEY, Ms Sarah, Assistant Secretary, Criminal Law and Law Enforcement Branch, Criminal Justice Division, Attorney-General's Department

CRAMSIE, Mr David, Senior Legal Officer, Telecommunications and Surveillance Law Branch, Attorney-General's Department

FRICKER, Mr David, Deputy Director-General, Australian Security Intelligence Organisation

GAUGHAN, Assistant Commissioner Neil, National Manager, High Tech Crime Operations, Australian Federal Police

KILEY, Mr Andrew, Senior Legal Officer, International Crime Cooperation Division, Attorney-General's Department

SENGSTOCK, Ms Elsa, Coordinator, Legislation Program, Australian Federal Police

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

CHAIR: Welcome. I reconvene the public hearing the Joint Select Committee on Cyber-Safety of the Commonwealth parliament for its inquiry into the provisions of the Cybercrime Legislation Amendment Bill 2011. Before I call representatives, can I just say that we are expecting some media. Has anybody got any objections to media being present? No. Everyone is happy with that. Thank you.

Although the committee does not require you to speak under oath, you should understand that these hearings are formal proceedings of the Commonwealth parliament. Giving false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. I remind you that the hearing is public. It is being Hansard recorded and it is also being broadcast live.

I will now ask you to make short introductory statements, and then the committee will proceed to questions. Can I just clarify: we have an hour between all three departments, so could you keep your introductory statements fairly brief because there will be questions from the committee.

Ms Smith: I think I am perhaps the only one who is going to make an introductory statement. I will ensure that it is short.

CHAIR: Thank you, Ms Smith.

Ms Smith: Thank you once again for the opportunity to appear before your committee and thank you for the opportunity for my colleagues from both ASIO and the AFP to appear also.

As the committee is well aware, the question of Australia's proposed accession to the Council of Europe Convention on Cybercrime has been recommended by the Joint Standing Committee on Treaties. This is the bill that is before the committee today. The Cybercrime Legislation Amendment Bill was introduced on 22 June 2011 and contains amendments necessary for Australia to comply with the convention's obligations and to deal with the general challenges associated with investigations in the cyber environment. Schedule 1 of the bill implements the convention's obligations in relation to providing for the preservation of stored computer data. It is the Telecommunications (Interception and Access) Act which currently regulates the access to stored communications. The access to such communications is under warrant, and carriers currently retain stored communications for as long as it is required for their own business purposes. However, in many cases, this is not

for a long period of time and, as a result, the preservation regime will allow a snapshot of target information while an investigation is on foot and before a warrant is obtained.

Preservation is designed to ensure that information that is relevant to a specific investigation is not lost as a consequence of the normal deletion process of information, which is different depending on which provider assistance is sought from. To obtain the warrant for this information it is through a Federal Court judge, federal magistrate or nominated AAT member. In the case of ASIO, it is the Attorney-General who would issue a warrant to access that information under preservation.

The bill also provides for the AFP to give notices to a carrier on behalf of a foreign law enforcement agency, with access to those communications being provided under mutual assistance. Schedule 2 of the bill deals with the mutual assistance aspects. Most of the amendments were contained in the exposure draft of the Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Bill, which was released for public comment in January 2011. These provisions will enable greater sharing of information between Australian and foreign law enforcement agencies. Schedule 2 of the bill will amend the mutual assistance legislation, the interception legislation and the Telecommunications Act to implement Australia's international cooperation obligations under the convention. Australia is already compliant with the majority of these international cooperation obligations under the convention, but the amendments in schedule 2 will ensure that all obligations will be able to be met.

Schedule 3 of the bill will ensure that the computer offences in part 10.7 of the Criminal Code Act 1995 are consistent with the obligations under articles 2, 4 and 5 of the convention. Schedule 3 does not introduce any new offences into the Criminal Code but removes the constitutional limitations in relation to the Commonwealth's heads of power. In the current form, the computer offences in the Criminal Code are restricted to conduct involving Commonwealth computers, Commonwealth data or the use of a carriage service. These limitations are not consistent with the obligations in the convention. Although state and territory offences provide some coverage for conduct which is excluded from the Commonwealth offences, there are still some gaps and to ensure that Australia can meet the obligations under the convention the schedule will remove the current restrictions on the computer offences in part 10.7 of the Code. The existing savings provisions in the Criminal Code will apply so that in the event of any inconsistency with state and territory laws, the latter will still be valid.

Schedule 4 of the bill makes amendments to ensure compliance with the convention's requirements to protect the confidentiality of the use of the powers under the convention. Schedule 5 of the bill makes two small changes to the interception act which are also necessary for accession. Item 1 of schedule 5 applies the necessary jurisdictional elements for the offences of unlawful interception and unlawful handling of intercepted information. Item 3 of schedule 5 amends the thresholds for access to non-content data on a prospective basis. The convention requires that the party's domestic laws cannot make telecommunication interception available to investigate a wider pool of offences than can be investigated with real-time traffic data. This is a technical amendment.

Finally, a lot of issues were raised during the hearing this morning and we heard those. We think it would probably be useful if we cut short our introduction and allow you to ask us questions on those many areas. We are very willing to participate.

Mr HAWKE: In relation to the issue about the definitions of telecommunications data and stored communications data, is there a reason these terms are not defined in the bill as it is currently proposed?

Ms Smith: The bill already relies upon the interception act, which has clear definitions of what is contained in a stored communications warrant. Telecommunications data is defined broadly under the Telecommunications Act because information is protected under the Telecommunications Act, and there are some other definitions. There are many different definitions of what is used under the convention that exists under the Telecommunications (Interception and Access) Act, but they are very different terms and the approach which is used to access them clearly defines what information can be accessed under that. One is content, in the case of stored communications, and one is non-content in relation to telecommunications.

Mr HAWKE: I understand that the current act has a definition, but I think the concerns revolve around the convention's definitions being different to what the bill would propose. Is that correct? It is using the term 'stored communications' as a catch-all rather than specifically defining what that refers to.

Mr Cramsie: The convention refers to different classes of information—that is, stored computer data and also traffic data. The way it translates into Australian law is that stored computer data are stored communications, essentially, and traffic data is the information protected by section 276 of the Telecommunications Act and also the non-content data access provisions in the Telecommunications (Interception and Access) Act. Whilst both the convention and the act use the term 'data', they are used in different contexts and have different consequences and thresholds for access.

Mr HAWKE: In relation to attempting to access a warrant or a preservation order, there is a contention that if this bill is passed in its current form there will be some sort of backdoor avenue for agencies to bypass the Telecommunications (Interception and Access) Act and seek this easier mechanism to gain the information they are after. Could both agencies respond to that?

Mr Fricker: The key issue there is that we still require a warrant. All the existing oversight mechanisms and procedural processes must be followed to obtain that warrant, approved by the Attorney-General, before we can actually have access to that information. That preservation notice would be given if we had formed an intention to obtain a warrant and we would like that data to be kept in its integrity prior to us obtaining that warrant. But we have no access whatsoever to that information until we have obtained the warrant. That warrant will have to be obtained under all of the existing mechanisms that exist today. There is no additional access to information. There is no backdoor in this. Under this bill, there is no informal way that we would have to obtain access to that information. We still require the warrant and there is no change to that warrant process under this.

Mr HAWKE: So there would still be the same threshold for the warrant?

Mr Fricker: Exactly.

Mr HAWKE: But the preservation would be under a weaker model; you could still require the carrier to preserve the data?

Mr Fricker: I do not know that I would use the term 'weaker'. It would still have all the formal arrangements.

Mr HAWKE: That is the contention that was put to us. That is not my language. It would be under a different threshold to the Telecommunications Act?

Mr Fricker: That is correct.

Ms Smith: One of the suggestions this morning was the possibility that a service would be the whole BigPond service, for example. That is not the case. It still has to be an identified service, being a phone number or an e-mail address, or something like that, as it is under warrant, and it has to be a person that you can currently obtain a warrant under. There still is the narrow scope of what can be applied for under a warrant. It would not be possible to determine that a service is the whole of BigPond; it has to be someone at BigPond. It has to be an identified type.

Mr HAWKE: I was not too worried about that. But in the specific case of a preservation order, that is under a different threshold to the Telecommunications (Interception and Access) Act is under. You are saying the warrants are the same system; applying for a warrant is the same under both pieces of legislation. It was put to us this morning that there is a different threshold for applying for both those warrants.

Ms Smith: No.

Mr HAWKE: You are saying that is wrong.

Mr Fricker: It is in the bill that we would not be able to seek preservation or issue that notice until we had formed the intention to raise a warrant—and this is from ASIO's point of view. That is where the two are interlinked. We must have a documented intent to raise that warrant, which in turn requires a security intelligence case to have been formed at some stage with us. The two are quite linked. Picking up on Ms Smith's point of view, it is not a case of putting in a weak preservation notice to preserve a whole range of information. We would only be seeking to preserve that information which is in the scope of our intended warrant.

Mr Gaughan: That is pretty much the same as law enforcement would operate as well. With the preservation order, all we are doing is seeking that the information be held by the carrier until such time as we are in a position to have obtained the lawful warrant by which we then receive the information. Preserve means exactly that; it means to hold it.

CHAIR: Is there a limit to the number of preservation notices you can have for each individual?

Mr Gaughan: There would be circumstances whereby one individual may be using multiple carriers. Therefore there would be an obligation on us to ensure that we had covered all those carriers. Does that answer your question?

CHAIR: There was contention earlier that you could just keep going with preservation orders and then it becomes interception. I am asking you to clarify whether that is possible or not.

Mr Fricker: In as much as for us to have intended to raise a warrant that sort of behaviour—just endlessly issuing more and more preservation warrants—would have no effect in terms of ASIO's security intelligence function if we never got access to that information. It would have no effect if we never did raise the warrant. If we ever did slip into that pattern of behaviour that would be under the scrutiny of the Inspector-General of

Intelligence and Security, who would rightly see that as improper conduct by ASIO, and that would fall within her reporting regime most certainly. I suspect that the ISPs would have an avenue to raise a legitimate complaint with ACMA and indeed with the inspector-general for that matter to indicate there is a pattern of behaviour here which is not in the spirit of the convention.

Mr HAWKE: With your dealings with carriers you are required to destroy data but there is no intent in this bill to clarify what happens with carrier data. Do you have a view on that? Your agencies are subject to this requirement and you are subject to scrutiny and other things but there is no intention in this bill. From a law enforcement perspective or otherwise, do you have any comments about that issue?

Mr Gaughan: We are comfortable with the current oversight regime. We do not see any need to change it.

Mr HAWKE: What about with what happens to the data at the carrier end? Do you have any concerns about that at all?

Mr Gaughan: We are fairly fortunate in this country that, as has been rightly pointed out to you, there are very good working relationships between law enforcement, the carriers and the Attorney-General's Department more broadly. We are comfortable with the practices that are in place with the carriers to ensure the privacy of the individual and also the integrity of the data.

Mr HAWKE: What do you understand happens with that data? What would your view be as an agency?

Mr Gaughan: I think that is probably best answered by the carriers.

Mr HAWKE: Do you know? Are you aware what happens to it?

Mr Gaughan: I am not aware.

Ms Smith: We are aware that the carriers are subject to the Privacy Act and as such information has to be protected. We also understand that they keep certain information for their own business purposes, which completely sits outside obviously law enforcement access. Our understanding under this new preservation regime is that, once the information is passed over to the agency if they obtain a warrant, then they should no longer have a need to have that information. They are likely to have passed over their only copy of it. We are not aware how they intend to do it in practice.

Mr HAWKE: Is there a specific requirement in this proposed legislation for them to destroy the data?

Mr Cramsie: Not in this legislation. Carriers that are bound by the Privacy Act are obliged to destroy information that they no longer have for the purpose for which it was collected.

Mr HAWKE: Does it mandate a time period?

Mr Cramsie: It is in connection with the initial reason why it was collected. If it is a situation where a preservation notice is revoked after a day, for example, a carrier may still need to retain that information for billing purposes or something separate. Whereas if it had been for a longer period of time then the provisions of the act will likely require that it be destroyed.

Ms MARINO: Should that be included in this legislation as well?

Ms Smith: It is certainly not a requirement of the cybercrime convention, which is the bill's main purpose. I think that is more a general question that needs to be looked at. It is not for the purposes of the cybercrime convention.

CHAIR: Preservation notices are only available for use where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. Is there a vulnerability test for preservation notices in the bill?

Ms Smith: No.

CHAIR: Should there be?

Ms Smith: I suppose the reason we have a preservation regime is that we have been advised by both industry and agencies alike that that data is vulnerable because it is destroyed for their own business purposes, which they have documented to us. That is why we need to ensure—not go on a cooperative basis, but actually have the legislation in place. I am not sure we are required. We understand that the provisions we have done are enough to comply with the convention, so we do not have a belief that we need to do anything further in that respect.

Ms MARINO: When a request comes through from a foreign source, is there any liaison between the Attorney-General's Department and ASIO, for instance, for the potential of any national security issues or other in the request that is being made?

Ms Smith: Do you mean under a formal mutual assistance request?

Ms MARINO: Yes, but even under the consideration that requests may well be made in the future that may contain essential elements of national security, depending on who it is targeted at. Is there normally a relationship or a contact between the two agencies in that regard?

Ms Smith: I might ask Mr Kiley to respond.

Mr Kiley: At the preservation stage that would not be required because that is on a police-to-police basis, so it would be a matter for the AFP to be satisfied according to the obligations set out in the draft legislation that the preservation is required. When the foreign country came to submitting a formal mutual assistance request to get access to either the non-content data or the stored communications data that had been preserved, if national security was an issue that is something that the Attorney-General's Department would follow up on.

Ms MARINO: But you could see no threat in the potential for a series of preservation requests leading to that point of view and exposing you before you get to that point?

Mr Kiley: No-one has any access to the information at the time it is preserved; it is only requiring the carrier to continue to hold the data. So there would be no implications of that until the foreign country made an actual request to access the data that had been preserved.

Ms MARINO: And then the contact is made and the assessment is made as to the intent of the agreement?

Mr Kiley: Yes.

Mr HAWKE: Turning back to ASIO, I want to ask a couple questions in relation to this bill. I have read through most of the convention. It is not about obligations in relation to intelligence gathering; it is about crime, obviously. So why is ASIO being extended the power to have preservation notices under this bill?

Mr Fricker: It really is on the principle that the additional security benefits that would be extended to, say, criminal investigations should be afforded to Australia's national security considerations as well. It is just the simple logic, if I could submit it to the committee, that it would not make sense to construct these arrangements in those regimes to protect one aspect of Australia's security while overlooking the opportunity it has to further ASIO's role in national security.

Mr HAWKE: They are interlinked; I understand that. I think these are simple questions, but do you have any limits to the number of preservation notices you can issue as an organisation?

Mr Fricker: It is related to the earlier discussion, I guess. There is no limit, any more than there is a limit to the number of investigations we might conduct or the number of warrants that we may raise. There is no numerical limit placed in legislation or statute anywhere, I think. It is entirely dependent on ASIO's pursuit of things of legitimate security concern.

Mr HAWKE: I understand. You gain access to the data via a warrant, as you have discussed. I think this question relates to Ms Marino's question about the operation of this through your agency. I guess the answer is via what you do, but how do you ensure that foreign policing agencies are not accessing data about Australians for intelligence purposes?

Mr Fricker: Through a police investigation.

Ms MARINO: Any form.

Mr HAWKE: Any form of request from a foreign agency.

Mr Fricker: That may be a question—

Mr HAWKE: I do not know if I expressed myself properly. What safeguards are there to protect Australian citizens from foreign intelligence requests in the guise of this convention?

Mr Fricker: To make sure that I understand the question, this would be a request made of ASIO through a foreign intelligence agency?

Mr HAWKE: No, even a mutual assistance request but through a foreign power seeking a preservation order.

Mr Fricker: I will speak to ASIO's part in this and then I might invite comments.

Mr HAWKE: I think it is important to what the bill is considering, because the potential for this is very much on the committee's mind.

Mr Fricker: At issue here is the step that we would have had to have formed an intention to raise a warrant. Raising a warrant, for ASIO, means it must be relevant to security under the heads of security defined in our act. Therefore it must be related to, for example, politically motivated violence, espionage, sabotage, communal violence et cetera. There are provisions for ASIO to undertake foreign intelligence collection warrants, but those are not at the request of a foreign agency; those are at the request of an Australian intelligence service. All of

these safeguards or thresholds, which are met prior to us having a warrant put before the Attorney-General and prior to the Attorney-General approving that warrant, must explicitly demonstrate a nexus to Australian security and must balance the protection of Australian privacy and human rights et cetera in the presentation and approval of that warrant. So there is no avenue here for any sort of foreign government agency to conduct a fishing expedition through some automatic process through ASIO. Nothing happens until we have that warrant approved, and there are quite specific requirements under the act. Essentially, it must have a nexus to Australian security; it cannot be to service another country.

Mr HAWKE: From your agency's point of view, you have these high thresholds to prevent that.

Assistant Commissioner Gaughan: I might add that what you are proposing, in theory, could be possible under the current mutual assistance request regime whereby we could have another country doing a fishing expedition.

CHAIR: I think that is the concern of the committee.

Assistant Commissioner Gaughan: As Mr Fricker has rightly pointed out, the information under this regime would be exchanged until such time as the MAR had been served. So this part of the legislation is a moot argument because it could already happen now. When we receive a MAR not only do we look at it holistically in relation to the privacy of the individual, plus a few other things we take into consideration, but also we look at the relationship we have with that foreign country and whether or not we think it is in the best interests of our organisation and the Australian community to cooperate with that MAR. There is nothing stopping us as an agency, in cooperation with the Attorney-General's Department, from not responding. So those safeguards already exist.

Ms MARINO: So within this bill you would still have the capacity to say no?

Assistant Commissioner Gaughan: Yes.

Mr HAWKE: You would be under the scrutiny of the Commonwealth Ombudsman in that regard. Would you then list those requests?

Assistant Commissioner Gaughan: We are under the scrutiny of the Commonwealth Ombudsman but we also have some internal governance around the issue of sharing information—it is a national guideline, no less. So the commissioner ultimately has oversight as well about what we are doing internally as an organisation.

Mr HAWKE: I am unaware of this in my reading of the bill, but is it required that you report on all requests to any agency?

Mr Kiley: For both access to stored communications and access to historical and prospective telecommunications data there is a requirement on the agency to report. For stored communications, the number of warrant applications that have been made and the number of warrants that have been issued and refused in response to those applications must be reported. Also, for telecommunications data there is an requirement on the Australian Federal Police to report on the number of authorisations they have made to disclose telecommunications data to a foreign country.

Mr HAWKE: Does that cover not responding to them as well?

Assistant Commissioner Gaughan: It technically does not cover not responding to them but we would certainly keep records of what we do not respond to through our normal reporting mechanisms, as we do annually for all our activities. If there was a requirement then we could put something into our governance instruments to ensure that was covered.

Mr HAWKE: One of these situations has been presented to us this morning where there was a disparity between Australian law and the law of another country for a particular category of crime. I am not thinking about a human rights issue or a violation, but more of a disparity in the severity of the sentence. What agency would be the first road block for that? Would it be the initiating agency?

Assistant Commissioner Gaughan: If it is police-to-police assistance it happens now on a daily basis in relation to what we do share and what we do not. As far as a mutual assistance request, it would come through the Attorney-General's Department.

Mr HAWKE: So it would go through you first? You would still say that you wanted it or it was a valid investigation and then you would go to the Attorney-General's Department and look at the different operation of the laws?

Mr Kiley: If a preservation request came in, that would go straight to the AFP on a police-to-police basis. If they assisted the foreign country and made the preservation order, and the foreign country followed up with a request to access the stored communication that has been preserved under the preservation notice, that will come

through the normal mutual assistance channels. The Attorney-General would consider the request, as is currently the case, under the Mutual Assistance Act, under the mutual assistance framework, with all the safeguards that apply, including dual criminality. So it would need to be an offence in Australia as well is in the foreign country. It would need to meet the penalty thresholds that are set out in the legislation. For stored communications, it needs to meet the three-year penalty threshold for us to provide the assistance. Once the Attorney is satisfied that it meets the thresholds set out in this amending legislation, as well as the safeguards already set out in the Mutual Assistance Act, the Attorney-General would have the power to approve the request, at which point it would go to the AFP or an enforcement agency to apply for a stored communication warrant.

Mr HAWKE: That was a good quick summary; that sounds reasonable. There are two issues coming out of that. I will come back to dual criminality but, firstly, why is the three-year legal barrier a foreign end in Australia? Is that a requirement of the convention? It has been put to us that that could be an Australian three-year minimum.

Mr Kiley: Sorry, could you repeat that.

Mr HAWKE: Is it a requirement of us signing up to this convention that we have to meet a three-year minimum, either Australian or foreign? It has been put to us this morning that it should be an Australian three-year sentence.

Mr Kiley: Firstly, the three-year threshold that has been set for access to stored communications for foreign law enforcement purposes simply accords with the threshold that applies for accessing stored communications for domestic law enforcement purposes. That is something Catherine might be able to speak more on, but a three-year threshold applies. In relation to the second part of your question, what you seem to be getting at is why we rely on a foreign penalty as opposed to the penalty that would apply to that conduct if it was committed in Australia. It is simply the penalty that applies to the corresponding offence—that is the way it works under mutual assistance at the moment. So all requests that Australia receives for assistance at the moment, be it for a search warrant or for other types of assistance that we can currently provide under the act, are in relation to the penalty that the offence attracts in the foreign country. So the current act applies to, say, a search warrant for a serious contravention in a foreign country, which is 12 months imprisonment or greater in the foreign country. That is the way mutual assistance works across the world; it is always in the requesting country, not the requested country.

Mr HAWKE: We have had some people suggest to us this morning that dual criminality can be circumvented in relation to this bill. I will try to get to the bottom of that, but it has been put to us that this could be overcome in the issuing of a preservation order. Does anyone have a comment or a view on that? Is there somebody who can explain that? There are two or three different things there.

Mr Kiley: I will start off and then I might pass on to Catherine to speak more about preservation notices where dual criminality does not apply—but there is a specific reason for that. In relation to access to stored communications and access to prospective telecommunications data, the foreign country can only access those types of data under a formal mutual assistance request, and all the safeguards set out in the Mutual Assistance Act that currently apply will apply to these new law enforcement powers for foreign purposes. So all of the grounds for refusal set out in section 8, including dual criminality, will apply to any request by a foreign country to access stored communications and prospective telecommunications data.

Mr HAWKE: Okay. Good. And in the case of a preservation order?

Mr Cramsie: The reason it is not catered for at the preservation notice stage is that the assessment of issues such as dual criminality and other factors that are appropriate under the Mutual Assistance Act is done in response to a request for mutual assistance. If those factors are going to be assessed prior to a decision about whether to preserve the information is made, you will have a time gap in which the relevant information will not be preserved. So the premise in relation to the Mutual Assistance Act is that you ensure the information is not initially deleted in that short period of time after you become aware that it may or may not be pertinent to the investigation, and then the safeguards that apply in the mutual assistance legislation will ensure that it is only disclosed in appropriate circumstances.

Mr Kiley: In addition to that, at the preservation stage, the foreign country does not have any access to the data that has been preserved. They only get access to the data once a formal mutual assistance request is made, and that is the appropriate stage at which to make the dual criminology assessment.

Mr HAWKE: And an agency requires a warrant.

Ms MARINO: In a practical instance, where a foreign country has received some communications information from their mutual assistance application and the act states, in 142A, that this can only be used for the purpose for which the foreign country requested the information in the first place, do you have any evidence, having had this happen previously, where the information is passed on for a secondary use? In the instance where

we will see a lot more of that, given the advances in technology, how would you see this being enforced and monitored into the future, especially with issues to do with commercial confidentiality and personal information or that of a national security basis?

Mr Kiley: As was raised this morning and in submissions, both for telecommunications data and for stored Communications data, when that is provided to a foreign country it can only being provided for the purposes for which the foreign country requested it. They can only use the data that was provided to them for those purposes and there is also a requirement on those countries to destroy the information that was provided to them when it is no longer required for the purposes for which it was provided to the foreign country.

Ms MARINO: Is that what happens? Can we be sure that that is what will happen, with increased numbers of requests and the fact that any country under this particular bill will be able to make that request? Can we and others have that confidence?

Mr Kiley: I think we can. It is the department's long-standing experience that undertakings provided and conditions imposed in the mutual assistance context are respected by foreign countries. Mutual assistance operates on the basis of reciprocity so if we ask other countries to only use information that we provide them for the purposes for which it was provided, it is our understanding that they respect that because if they do not respect those conditions, we will not be in a position to help them in the future. In the same way, when other countries provide information to us we undertake to use it only for the purposes for which we sought the information.

Ms MARINO: Has there been an instance where that has not been the case?

Mr Kiley: Not that I am aware of.

Mr Gaughan: I am not aware of any either. The answer is 100 per cent correct. We are already sharing information with international law enforcement through MAR on pretty much a daily basis. If they do the wrong thing by us then the relationship we have with those countries obviously is not there anymore and there will not be that same assistance on a police-to-police basis. Not only is the MAR process in place but we also have a large number of MOUs with foreign law enforcement which are signed commissioner to commissioner with the understanding that that information is used only for the purposes it was requested for. As much as we can be confident that another law enforcement agency will treat our information in accordance with our own laws we are but I do not think, from a police perspective, that I can give a 100 per cent guarantee that that is going to be the case. Rest assured that, if they breach our trust, the relationship will sour to the extent that we will not be assisting in future.

Ms MARINO: Back to the practical end of the internet service provider, we have a whole different range of sizes of these which may or may not be captured by this. Once you put in a request for a copy, a copy will have to be made, which means that there are those within that environment who may have access to that information. In relation to security at that level, what would you suggest within the legislation that could improve that?

Ms Smith: We already have the assistance of the telecommunications industry for interception at a very high level—that is, access to information over a period of days weeks or months, depending on the interception warrant. Obviously they already assist with the execution of stalled communication warrants and they also give assistance and access to data. Most providers we deal with will have units within the carrier or the ISP whereby they are personnel we deal with from a law enforcement and national security perspective and they are trusted people. There are exceptions in the legislation that allow providers access to information for their general business purposes and to execute warrants and things like that. There certainly are already prohibitions in the act and exceptions in the act which allow them to do this.

Mr Fricker: As Ms Smith just said, ASIO has long-standing relationships with ISPs to deal with very delicate matters to do with our interception warrants. We security clear I SP staff, so within organisations there will be individuals who have passed a security clearance process from the federal government sponsored by ASIO. So there is that level of trust and a whole regime behind that to ensure that individual's privacy is being protected and that the conduct and the handling of that information is being performed properly.

Ms MARINO: Does that extend to all of the ISPs that will be picked up under this particular piece of legislation?

Mr Fricker: I will just check in a moment at what sort of coverage we have. But certainly this falls into the long-term practice. ASIO already has interception powers—I am stating the obvious here.

Ms MARINO: Absolutely; I understand that.

Mr Fricker: So all we are talking about here is extending this capability for these preservation orders. The business of intercept, the business of handling that and the business of having an ISP's cooperation in ASIO

operations is a long-established practice. So there is a whole tradition of procedures around that to protect the interests of all involved. I might just double-check.

Ms Smith: Another point is that the main area where information is being destroyed in a very short period of time is, without doubt, the large mobile providers of which, in fact, there are very few in Australia. Excellent arrangements are in place for those who are beyond reproach. There are also provisions in the interception legislation that requires them to build certain things to protect that information. All information about stored communications has to be protected under the act. So any provider we deal with is very much made aware of those provisions. There is a very high level of trust and satisfaction given that they will protect that information. All carriers—I think there are 160-odd at the moment—are required to lodge interception capability plans on an annual basis and, in doing that, they will advise us of the personnel who can be dealt with on these issues. They certainly take their responsibilities very carefully, they tread very carefully and they give us information we need to get a certain level of assurances.

Mr Fricker: Just to finish off that last point, we cannot have security clearances active for every ISP operating in Australia. However, we do have security clearances for a large number of those ISPs, a large number of the business that we have for the ISP community and where we are not able to maintain security clearances because of the churn or the reach into the organisations we take whatever measures we can, such as confidentiality agreements, as well as the range of measures that Ms Smith just went through. I add that for clarification.

CHAIR: I want to go back to the issue you were talking about with the ISPs. We heard earlier that it may take some time, certainly for Telstra, to design, build and deploy necessary equipment and make the network and IT systems changes. I wonder whether you think that is correct. Do you have a view on that and, if so, please say so. As I understand it, once the legislation receives assent they say they may need up to 18 months, not 28 days, to get everything in order. I wonder whether there is any scope in the legislation for anything like that?

Ms Smith: I was quite surprised when I heard that this morning and when I read the submission. We have been working for some time with the main players, as I said earlier, who actually provide mobile services like text messages of where the high risk is of losing that evidence or intelligence where it is needed. In fact, those particular providers have sought to have clarity in the legislation about this obligation so they actually had a business purpose to hang on to communications that they may be destroying for business purposes at the moment. My understanding is that they were assisting law enforcement to preserve information where they anticipated a stored communication warrant for a very serious offence—for example, if someone has been murdered and they have a phone number and are worried about the destruction of evidence. They had already been doing that.

The act and the convention do not require stored communications to be provided in a specific way. They do not require any capability. We use language like interfaces—I am not an engineer—delivery, all these things, which is very definite language that we use in relation to intercepting capability. For interception capability they do have to be compliant with requirements under the act. That is not the case with these preservation requests. I think the convention already refers to not requiring industry to go outside their particular practices. In my discussions with them I have been extremely flexible with it and said, 'We think any way you can manage this will be a good thing.' It may be in the case of a small ISP, for example, that they copy some emails onto a CD-ROM, lock it in a protected filing cabinet and then, when the warrant comes in, that is what they hand over. There is no perfect science on how this will actually be done. Certainly we are willing to talk to industry now and are talking to industry about their obligations on a daily basis as to how they can do this to best have it up and running.

I suppose in reality, for the convention's purposes, to be compliant and to accede to the convention, the legislation would need to be in place. So I think it is important that we start talking to industry very quickly on how this will be done. I suppose it was some level of surprise for myself, because I did not understand from my discussions that there would be any need to build delivery standards or have any specifications or anything like that. We are not going to tell them how to do it; we want them to tell us how it is best done. There are already delivery systems in place for the delivery of this kind of information—the stored communications regime.

CHAIR: I put that to Telstra. I asked, 'Don't you already have to do this anyway?' They could not actually tell me that there was going to be X amount of an increase in the workload. That is why I have asked the question, just for some clarification.

Ms Smith: I should also say that the Telecommunications Act is being amended to ensure that they will be able to recover costs for foreign preservation notices and of course for the domestic ones as well, for giving that information, storing that information, passing it over.

CHAIR: To move on to another area that came up earlier with regard to safeguarding privacy, I think the Australian Privacy Foundation were talking about section 180F. Schedule 4 introduces confidentiality provisions to make it an offence to disclose information about authorisations. I am wondering what your comments were. Did you see that this morning? Are you aware of what I am talking about?

Ms Smith: I heard a little bit but I am going to throw to my colleague David, who was here throughout it. Essentially there is a requirement in the legislation at the moment, the TIA Act and the Telecommunications Act, to protect this sort of information. This is extending those protections onwards and also relying I think upon the cybercrime convention's very strict safeguards and human rights compliance.

Mr Cramsie: There were the privacy aspects in relation to keeping confidential the authorisations that are made under the convention.

CHAIR: And then when the people are told at the end, if there is no issue involved, whether they have been subject to collection.

Mr Cramsie: In relation to the first aspect as to why that is being made, it is a requirement of the convention that the use of powers that are made available by it are done so in confidence. At the moment under the interception act the exercise of telecommunications interception warrants and stored communications warrants are treated with such confidence and it is an offence to disclose the existence of them. The purpose of schedule 4 of the bill is to extend that to the authorisations that are being made to disclose the existence of authorisations to disclose telecommunications data. That serves two functions in relation to consistency throughout the act and also compliance with the convention's obligations. In relation to a general notification requirement, I think Ms Smith will talk about that.

Ms Smith: That issue is more about the act as it sits at the moment. If interception of a person's data is sought, there is a question of whether they should be informed at a point where the information is no longer of use or the investigation is not proceeding. That is a very big policy question and certainly not something the department has a view on. I am aware that the only jurisdiction that I have ever heard of that does it is the USA, and they do not do it in all cases. They only do it where there are innocent parties to a communication, because they have a minimisation process whereby you are not supposed to intercept innocent parties to communications—some years after, apparently. I have been told it is not an instantaneous thing; it is many years after the fact that they will do it. I think that is more a matter for government. That is a question on the act itself as it stands at the moment, because the information is currently collected under the act. It is certainly not relevant to the convention.

Ms MARINO: In the WA state government's submission, they referred to the minister's speech talking about any inconsistencies between Commonwealth and state or territory laws and saying that the savings provisions in the Criminal Code ensured the validity of those laws. But the WA state government was really concerned about direct inconsistencies that could be subject to section 109 of the Constitution, where federal laws would overtake state laws. Where do you see that in relation to the criminal offences for computer crime in Western Australia? Where do you see their laws in relation to this particular piece of legislation?

Ms Chidgey: It is the case at the moment that the Commonwealth computer offences as they currently stand overlap very significantly with laws in every state and territory. The changes that we are making as part of this bill only very incrementally expand Commonwealth offences. Since 2001 the Commonwealth has had offences in this area and had a savings provision, with both the Commonwealth and states taking action under those offences. There has not been an issue to date. There are some cases before the High Court about coexistence of concurrent criminal laws at Commonwealth and state level. The effect of the bill will be very minimal on Commonwealth offences, because at the moment we cover every computer offence that occurs using a telecommunications service, which would be almost all of them. There is only a small gap in relation to offences that do not occur over the internet. An example might be if someone put a virus on a computer using a USB stick rather than doing it on the internet. But that would be a very small proportion in terms of the new area that we would cover as a result of this bill. The Commonwealth's longstanding position covers quite a number of offence regimes—drugs, money laundering, computer offences—where for decades we have had overlapping offences with states and territories and we have always had savings provisions like we have in this instance, and there is no High Court authority yet that has suggested that those offences cannot coexist with savings provisions in place.

Ms MARINO: By that you are saying that the Commonwealth's laws would basically not override the state laws in that sense?

Ms Chidgey: That is right. Our approach is that we have done everything we can to preserve the concurrent operation of all the state and territory laws.

Ms MARINO: Is there any chance that section 109 could override those state laws?

Ms Chidgey: There is a case before the High Court at the moment, where a ruling is expected in coming months, and that may have further developments, but it would be impossible to speculate. I guess our view is that this bill does nothing to change things, in that the Commonwealth law overlaps with state and territory law almost entirely at the moment. Of all offence regimes, computer offences are an area where the Commonwealth has, I guess, a natural reason to be there, both because of the telecommunications cross-jurisdictional angle—and we have clearly got a telecommunications power in the Constitution—and the international angle, which means that it is inevitably an area where the Commonwealth will have to play a lead role.

Ms MARINO: So, effectively, on the constitutional matters, the Commonwealth law would override the state's law if it came to that situation?

Ms Chidgey: It is impossible to speculate. That has not been the case to date, and offences have operated concurrently in state and territory law for decades, as I said. The current judicial position would be that they can coexist.

Ms MARINO: Depending on the outcomes we see in the High Court, can you see any implications for that in relation to this particular bill with state rights and state laws?

Ms Chidgey: No. As I mentioned, the changes that we are making are a very small, incremental expansion that would affect a very limited number of offences. In a worst case scenario, where the High Court found that the Commonwealth and state offence regimes covering the same subject matter were slightly different, it would mean the Commonwealth and the states and territories having to consider their approach across all drug offences or money-laundering offences—a whole range of areas. The change that this bill is making in computer offences is a very, very small change, so I do not think this affects that position at all.

CHAIR: Just before we finish, I want to go back to the privacy test under section 180F of the bill that directs an authorising officer to have regard to the affected person's privacy. A few submissions today have told us that is vague and meaningless. I am wondering if you have any reason for using those words, and if you think that the provision could provide clearer direction, especially to the police, in regard to that?

Ms Smith: It is the language that is already used in the legislation in relation to access to prospective data, which is information that is non-content information that is obtained on a prospective basis. We believe it is an appropriate proportionality test. The act, in effect, prohibits access to any communications, and then access has to be on the basis of lawful authority. That now, including this in this case, will mean that every type of access done with that has a privacy question in it. We consider that it is consistent with what is currently used in other parts of the act, and from our understanding—and certainly the AFP might have something to say on this—they do consider the privacy versus the law enforcement need. There is a balance test done on every occasion, but that is obviously done internally. The language is strictly because it is the language that is consistent with what is already used, rather than bring in too many new definitions.

CHAIR: Is the language consistent with the convention?

Ms Smith: There is requirement to have consideration of privacy in the convention, and the whole TIA Act considers privacy.

CHAIR: Is that likely to prove any problem when assisting foreign law enforcement agencies?

Mr Gaughan: No, Chair.

Mr Fricker: Chair, very briefly, I would like to make one final submission. We have, quite properly, discussed here this afternoon many aspects of the safeguards and the proper conduct of these provisions. I also submit that if we do not make these changes, certainly in ASIO's case, we will fall behind our ability to provide a picture of the threat environment facing Australia, particularly around terrorism and espionage. There is no aspect of those investigations that we conduct that does not have some element of a telecommunications or cyber component to it. The time frames and the technology and the business models of the ISPs are such that I can guarantee this committee we will miss valuable intelligence around those areas of espionage and terrorism unless we have some mechanism of keeping pace with technology. Again, without taking the time of the committee too far, I make that submission to the committee—that is, not only, in my opinion, are adequate safeguards being built into these arrangements, it is in fact essential for Australia's security to advance with these sorts of reforms.

CHAIR: Thank you. And I thank you all for attending the hearing today and giving your evidence. Your participation has been a valuable contribution to the inquiry, and the secretary will contact you if the committee has any further questions.

Resolved (on motion by **Mr Hawke**):

That this committee authorises publication of the transcript of the evidence given before it at public hearing this day including publication on the parliamentary electronic database of the proof transcript.

Committee adjourned at 14:28