



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE

Reference: Cybercrime Bill 2001

THURSDAY, 9 AUGUST 2001

CANBERRA

BY AUTHORITY OF THE SENATE

WITNESSES

CHIDGEY, Ms Sarah Jane, Legal Officer, Attorney-General's Department..... 52

**McDONALD, Mr Geoffrey Angus, Assistant Secretary, Attorney-General's
Department..... 52**

TAYLOR, Mr Gregory Charles, Vice-Chair, Electronic Frontiers Australia 45

SENATE
LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
Thursday, 9 August 2001

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

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

Senators in attendance: Senator Payne (*Chair*), Senators Cooney, Mason and McKiernan

Terms of reference for the inquiry:

Cybercrime Bill 2001

Committee met at 5.34 p.m.

TAYLOR, Mr Gregory Charles, Vice-Chair, Electronic Frontiers Australia

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

The Senate referred the bill to this committee on 28 June 2001 for inquiry and report by 21 August 2001. The committee advertised the inquiry on 7 and 8 July 2001 in the *Australian* and received 24 submissions in total. The first hearing on this bill was held on 19 July, and this is the second and final hearing. I note for the record that this committee meets this evening at the pleasure of the Senate, which grants us permission to do so, and the Senate is in session. If we are called to the chamber, there may be some interruption to the proceedings. I ask witnesses to bear with us in that regard.

Welcome, Mr Taylor. Electronic Frontiers has lodged a submission with the committee, which we have numbered 15. Do you have any amendments or alterations that you want to make to that submission?

Mr Taylor—No, but I would like to state that, due to the pressures of time, we were not able to address every aspect of the bill in our submission. If we had the chance, we would have addressed some of the other issues. We are aware that other organisations have addressed in their submissions issues such as definitions and the security aspects of the bill. It should not be taken that our omission to address those issues means that we are totally satisfied with those aspects.

CHAIR—We note your clarification there. I invite you to make a short opening statement. At the conclusion of that I am sure there will be questions from members of the committee.

Mr Taylor—Our submission contains detailed commentary on certain provisions in the bill, and I will not detail those issues now. However, I would like to make some brief opening

remarks. I appear today as an advocate for a balanced approach to law enforcement that takes civil liberties into account. I am also a practising IT professional with computer security responsibilities. An important issue is what constitutes cybercrime. Do we mean crimes against computers, traditional crimes that happen to be perpetrated using computers or both?

The committee previously has queried the global annual cost of cybercrime of \$3 trillion, as quoted in the second reading speech. This figure appears to have originated from a report by *Information Week* in July 2000, which estimated that annual cybercrime costs were \$US1.6 trillion. However, this figure is an extrapolated estimate largely based on the estimated productivity losses arising from eradicating computer viruses. Technically, most of the recently publicised attacks are worms rather than viruses, but I will use the term 'virus' here because it is perhaps more widely understood.

One might easily be led to believe that the estimate of \$3 trillion was actual losses incurred through funds stolen or otherwise fraudulently obtained, but this is not the case. Perhaps cyber vandalism might be a better term for this type of crime. Most such losses go unreported, presumably because it is an embarrassing admission of lax computer security measures. While there are undoubtedly costs associated with recovery from the virus intrusion, the prevalence of successful attacks of this nature would be greatly reduced if more attention were paid to IT security in both private sector and public sector organisations.

A further problem is that software released by Microsoft, the most commonly used software worldwide, is all too frequently vulnerable to attack and, even worse, is released with low security settings as the default configuration. The recent outbreak of the code red worm, which exploited a vulnerability in Microsoft's flagship web server software, is a case in point. Wild estimates of damage from this attack have been made, but the facts are that the vulnerability and the fix for it were well publicised over a month ago and the problem was avoidable.

The costs of good security are no doubt considerable, but they are a necessary cost of due diligence. It is better to invest in good locks for the doors than to complain about losses from a break-in. The bill currently under consideration will do little, if anything, to address the problem of computer viruses. In fact the immediate source of a successful virus attack may be a long way removed, both geographically and generationally, from the original perpetrator.

My point is that there has been a great deal of obfuscation and precious little detail made available about the actual problems this bill is meant to address. Vague and unexplained loss estimates of trillions of dollars do little to engender confidence that an understanding exists either in government or in law enforcement about how the measures in the bill will assist in successfully prosecuting actual computer crimes.

The committee has heard from a previous witness that the recently enacted New South Wales computer offences are the same as those in this bill. We would dispute that. There are several important differences between the Commonwealth bill and the New South Wales legislation. The New South Wales act follows almost exactly the Model Criminal Code while the [Cybercrime Bill 2001](#) features some questionable changes that have not yet been explained in either the second reading speech or the explanatory memorandum. These are described in detail in our submission, and I will not go into them at this point. Our other major concern is with law enforcement assistance provisions, which we believe infringe the right to silence and may lead to prosecution of the innocent and the possibility of inadmissibility of evidence so obtained.

EFA support in principle the implementation of laws to combat genuine computer crimes. However, we have reservations about the apparent haste with which these measures are being

implemented, especially as this will make Australia one of the first countries in the world to introduce computer offences based on the draft European convention. We would prefer to see a longer period of community consultation than is possible within the short time frame allocated to the committee's inquiry. As a minimum we would recommend amendments to the bill to at least bring it into line with the model code. However, our preference would be for a thorough and independent review of the model code to address the concerns that have been raised in our own submission and those of other organisations and individuals.

CHAIR—One of the witnesses we were hoping to ask some questions of but who is unable to be here today is the federal Privacy Commissioner. There is good reason for that, so that is not a problem, and we can certainly follow this up by way of correspondence. But do you think there is a need for overall privacy guidelines in the implementation of laws of this sort?

Mr Taylor—Certainly privacy guidelines, as expounded in the national privacy principles, are already available and will be implemented as part of the Privacy Act amendments which come into force in December of this year. We have not specifically addressed those issues in relation to this bill and I have not had the privilege of reading the Privacy Commissioner's submission. So I have to say that we have not specifically looked at those aspects. We do have some concerns though about the law enforcement assistance provisions in relation to privacy and security of data.

CHAIR—I think you recommend that they should be set aside until there has been a fuller exploration—

Mr Taylor—A fuller examination of the ramifications of what appears to be a fairly limited explanation both in the explanatory memorandum and in the bill itself about how these assistance provisions would be implemented in relation to problems such as were addressed in the United Kingdom RIP Bill. A great deal of concern was expressed about forcing people to reveal encryption keys and no real attention was given to the problem of someone proving they had forgotten their key—in other words, how you prove a negative. Issues like that really need to be thoroughly addressed. This is a fairly controversial measure which does not seem to have been highlighted as such in the second reading speech.

Senator McKIERNAN—From your comments it is obvious that you have read the *Hansard* of the committee's first hearing in Sydney a couple of weeks ago.

Mr Taylor—Yes.

Senator McKIERNAN—You make a comment in your submission about the responsibility of legislators to create law that is unambiguous. That comment comes under 478.1—unauthorised access to, or modification of, restricted data. I would ask similar questions in relation to the definitions in the bill of computers and computer databases which were recommended in the Model Criminal Code report. Would you have a view, in light of the questions that were asked at the previous hearing and your comments today, that the Commonwealth is abdicating its responsibilities in this whole area? Or do you have a more narrow view than that?

Mr Taylor—In terms of definitions?

Senator McKIERNAN—Yes, indeed.

Mr Taylor—The problem with definitions, particularly of a computer, has received a fair bit of attention both in the report of the Model Criminal Code Committee and in submissions from others to this committee. We understand the problem—if you define computers too narrowly, you may be omitting potential offences either now or in the future. If you define it too widely, you tend to take in offences that are relatively trivial and should not be

prosecuted. We do not have a particular problem with omitting the definition of a computer within the bill, although obviously it is reliant on the courts to interpret what the current everyday meaning of the term 'computer' is.

Senator McKIERNAN—Ultimately, there will be a definition, which will be done by the courts, won't it?

Mr Taylor—It may be done by the courts on a progressive basis. As technology advances, it is up to the courts to interpret what was the intent of the parliament at the time.

Senator McKIERNAN—You make the comment about the responsibility to create laws under the 'unauthorised access to, or modification of, restricted data' heading. Why do you think the Commonwealth is abdicating its responsibility in this area?

Mr Taylor—I am not sure that I use the term 'abdicating responsibility'. In general, the comment that has been received on the bill, both in submissions to the committee and in the media, is that definitions of the offences are very broad. The question arises as to whether the parliament should narrow the terms of the definition of the offences so that it is made quite explicit as to what is covered. I believe mention was made at the previous hearing about the fact that computers exist everywhere these days—they are in the home, they are embedded in microwave ovens, they are in mobile phones, PDAs, et cetera. Really, the intent of this bill is to determine which of those particular types of devices are meant to be covered in terms of what we are calling cybercrimes.

Senator McKIERNAN—You expressed some concerns about Australia being the first country to adopt the European convention—it has not yet been adopted in Europe. Indeed, the convention has not yet been formally endorsed. It is still in the development stage. What dangers do you see in Australia going down this route and being the first to do so? Obviously there is a need for some form of legislation in this area. We have got to have some model somewhere. Is it not a good idea to use this as a starting point for the development of legislation rather than the Model Criminal Code recommendations?

Mr Taylor—The European convention has been fairly controversial, not only in the definition of the offences but in relation to the law enforcement provisions. This particular bill utilises the definitions of substantive offences from the European convention. It does not go nearly as far down the track of law enforcement provisions. Our organisation has in fact been involved with the European convention by way of participation in a group of like-minded organisations around the world which have submitted submissions to the committee that was developing the draft convention since it became public in April last year. The result of that was that we were able to effect some changes to the European convention by way of recognising privacy rights and human rights generally. We and other organisations like us around the world are not happy with the current draft, which is basically the final draft of the committee before it goes to the council of ministers.

Whether Australia should be taking a lead in being one of the first to implement these particular elements of the convention is something we would have some concerns about. We think it might be better to let other countries implement these offence provisions first and find out what kinds of legal problems arise. We do not think Australia is particularly well regarded internationally in terms of its understanding of technology and the Internet. We have had concerns in the past about this government's censorship legislation and the digital television legislation, as examples, which we do not think were particularly well handled and tended to make Australia something of a laughing stock internationally. We do not think this bill will quite have that effect but it is a fairly brave step to go out and be the first country to

implement these offence provisions and therefore have to deal with the potential legal problems that arise.

CHAIR—Thanks, Mr Taylor. I just wanted to pick up one point before I turned again to my colleagues. Have you had the opportunity to look at the Australian Computer Society's submission on this bill?

Mr Taylor—Yes I have.

CHAIR—They also mention the point which you make on page 3 of your submission about the definition of telecommunications service. You note that it looks as though the proposed legislation narrows the Model Criminal Code paragraph on unauthorised access to or modification of restricted data by confining it to 'Commonwealth computers or computers accessed by means of a telecommunications service'. You go on to say that that definition is a particularly broad one—a point also made by the ACS. That is a concern in your view because of the breadth of activity that can be brought in. Is that your particular concern?

Mr Taylor—Yes, that definition comes from the Telecommunications Act, which was established some years ago, and developments in technology since then have meant that networks are everywhere. Even in the house you can have your own telecommunications network, effectively, which I believe would come under the definition of telecommunications. I am certain the bill itself is not meant to cover intrusions by siblings into other people's computers in the domestic environment. That is one of the issues that needs to be addressed as to exactly what is the coverage of this bill. It does not seem to be very well described in the face of the bill.

CHAIR—Thank you.

Senator COONEY—As I understand it, the legislation is attempting to stop people doing things to computers. There will be some things you will be able to do to computers which are legal and there are some which are illegal. This legislation is after the illegal actions that result in troubles for computers. Is that right?

Mr Taylor—I think the term used in the bill is 'unauthorised' but it goes further than just modification of data; it covers access to information within a computer. That raises the issue of why we particularly want to criminalise access to information just because it is in a computer if there is no damage done. We do not have similar offences for information that is stored in a filing cabinet, for instance.

Senator COONEY—There are some penalties of 10 years and others of two years. Have you looked at that? I am trying to understand whether the penalties are out of proportion to what is happening, or not.

Mr Taylor—I think the problem is that the bill does not necessarily require that any damage or harm be caused in relation to any unauthorised intrusion. We think that is a departure from traditional approaches to criminal law in relation to property in that mere access to information can result in a huge penalty by way of a prison term, without there being any malicious damage involved.

Senator MASON—I understand your point about damage and, as you said on page 1 of your submission, that penalties are perhaps too high:

... as many of the offences proposed do not require an element of damage, physical or monetary ...

Isn't the criminal law about, even more than damage, potential damage? That is why in the law—remind me, Senator Cooney—of attempt there might be no damage but the offence may still be extremely serious. Isn't that the key here?

Mr Taylor—It is.

Senator MASON—Isn't that why the penalties are so high?

Mr Taylor—Yes, but I think it raises questions about how one proves what the potential damage might have been in relation to these types of crimes.

Senator MASON—That is a fair point and I accept that. Potential damage is always an issue for evidence, but as a matter of principle I think that what Senator Cooney was getting to was that penalty in the criminal law relates very much to potential damage. The law of attempt is a classic example of where it is all about potential damage. I accept that there may be problems of evidence in determining what is the potential damage but I think the legislature here is trying to focus on potential damage. I say that because I think that is the issue.

Mr Taylor—That is certainly what that law seems to be aiming at. The question is: how practical is it to prove in a court of law what the potential damage is or what the intent of the perpetrator was? We have no problem with a law that says that, if you cause damage that causes loss to some organisation, it is a major criminal offence depending on the size of that loss and so on. When you move into potential damage it becomes a rather difficult concept to grasp, I think, in this particular instance.

Senator MASON—It becomes more difficult as a matter of evidence but not as a matter of principle. Anyway, I have made my point. Thanks.

Senator COONEY—I will go to another issue. Can these offences be committed from overseas? You are talking here to somebody who is not as *au fait* as he should be with computers.

Mr Taylor—The development of the Internet means that every computer that is connected to the Internet is potentially connected to every other computer. Unless there are adequate firewalls in place that protect computers in a particular organisation then it is possible to penetrate those computers from anywhere; it makes no real difference whether it is from next door or from the other side of the world.

Senator COONEY—So there would be a large scope for the use of extradition proceedings? You might not have fully looked at that.

Mr Taylor—Certainly cooperation between different countries and agreement on common offences between different countries has to be a key element of this type of law, and that is in fact what the European cybercrime convention has attempted to address.

Senator COONEY—Thanks very much for that.

Senator MASON—Mr Taylor, on page 4 of your submission you speak about schedule 2, 'Law enforcement powers relating to electronically stored data.' In the third paragraph you say:

The proposals in the Bill are indeed controversial. The matter of assistance orders is aimed squarely at the problems presented by security passwords and, more particularly, encrypted data.

It strikes me—and I do not know; I may ask Mr McDonald later on about this—as an unusual departure, as a matter of principle, to have in a criminal law matter what they call assistance orders to, in effect, force cooperation. Is this unusual?

Mr Taylor—There are other federal laws, particularly I believe the Corporations Law, that do require assistance orders. I do not know a lot about that particular law but I understand that where such assistance orders are invoked we are generally talking about serious crime. This

bill does not really specify the circumstances in which an assistance order might be granted; it only requires a magistrate's order to invoke this particular provision.

Senator MASON—Is your objection one based just on privacy?

Mr Taylor—Privacy is one issue. If in fact there was definite evidence of a serious offence that required access to encrypted data, we would not see any major problem with that. But the bill does not specify the nature of the offence or whether other evidence is already available that suggests that there is information, in an encrypted form, that might be used as evidence.

Senator MASON—Schedule 2, then, is too broadly cast? Its net is too broad and therefore the balance between law enforcement and privacy is out of kilter?

Mr Taylor—Yes. As it stands the bill says that an order must be complied with, otherwise there is a prison term involved. It could well be that someone has forgotten an encryption pass phrase, but how do they prove that? This was the issue that was raised many times in relation to the UK bill and eventually some watering down of the provisions of that was done. But it is still an issue that has to be addressed; it cannot just be slid under the carpet.

Senator MASON—I understand. We might be able to ask the Attorney-General's Department about that shortly. Thank you.

CHAIR—Mr Taylor, thank you very much for assisting the committee with our deliberations this evening. We may or may not end up with further questions out of our examination of the Attorney-General's Department after this, which we may wish to seek some information from EFA on. If so we will do that quickly and by correspondence, and any assistance you could give us in responding to that would be appreciated. Is there any final comment that you wish to make?

Mr Taylor—No, thank you. We would be happy to assist you in any way that we can.

CHAIR—Thank you.

[6.05 p.m.]

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

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

CHAIR—Welcome. The department has provided answers to questions which were taken on notice from an earlier hearing, and we have listed those as submission No. 20. Thank you for those responses. I invite you to make an opening statement at the conclusion of which I will seek questions from members of the committee. You will not be asked your views on matters of policy or reasons for policy decisions. If it is necessary we will give you the opportunity to refer those matters to the appropriate minister.

Mr McDonald—Thank you. Rather than giving a general opening statement, I will touch on some of the more important issues that were raised in some of the written submissions. We will also provide this in writing, and we will do it very quickly because I understand that you have very little time to finalise the report.

CHAIR—We have a reporting date of 21 August.

Mr McDonald—The first issue raised that we would like to touch on is in the submission of the legislative subcommittee of the New South Wales Society for Computers and the Law. There is a little overlap between the various submissions at times, so we will try to hit on the various topics. One of the issues was a concern about the impact of this on copyright law. The subcommittee asserts that the proposed new computer offences in the bill will create an alternative regime to the laws relating to copyright and greatly expand the protection of data beyond that contemplated by the Copyright Act 1968. We are confident that the [Cybercrime Bill 2001](#) will not affect the copyright law regime. Firstly, the conduct described in many of the subcommittee's examples would not constitute offences under the proposed legislation. The proposed offences apply only to conduct which affects Commonwealth data or involves the use of a telecommunications service. Modifying the switches in a DVD player, which is one example, or accessing a data set using the incorrect software does not affect Commonwealth data or involve the use of a telecommunications service, and this conduct is not covered by the proposed offences.

Secondly, these offences deal with access to data which is unauthorised, and the sorts of situations there that have been raised would suggest that we are talking about something that is authorised. Finally, even if there were some glimmer that one of these offences could apply, where a person accesses restricted copyright material for a permitted purpose within the terms of subsection 116A(3) or 132(5F) of the Copyright Act 1968, the defence of lawful authority, which is in section 10.5 of the Criminal Code, applies. Section 10.5 of the Criminal Code provides that a person is not criminally responsible for an offence if the conduct constituting the offence is justified or excused under a law. So it does not have to be something absolutely spelt out in that law. If it is under that law then you are not criminally responsible. Subsections 116A(3) and 132(5F) of the Copyright Act allow the use of a circumvention device to be supplied to a qualified person for use for a permitted purpose. As the Copyright Act suggests, there is permission for qualified persons to use circumvention devices in accessing copyright material for a permitted purpose. Where it is authorised, such persons would be able to raise the defence of lawful authority in a prosecution for unauthorised access to restricted data.

The whole way this Criminal Code is organised and the whole point of that lawful authority defence in 10.5 of the Criminal Code is to allow schemes that have been thought

through in relation to specific areas of regulation to operate in the way they were intended. Of course, a director of public prosecutions, when deciding whether to prosecute, is very conscious of what the obvious defences are. This is an obvious defence. Historically, the idea of there being a lawful authority defence, which is in 10.5 of the Criminal Code, is not unusual. The only thing with it, of course, is that the Criminal Code lawful authority defence is actually a bit easier to establish for the defendant than some of the old provisions. One of the old provisions was 15D of the Crimes Act, which had a legal burden of required proof on the balance of probabilities of the defence. Under the code it is an evidential burden. Section 13.3 of the code provides that the person would simply have to point to some evidence to demonstrate that he or she had some lawful justification or excuse under that law. There is nothing to be concerned about in relation to that aspect of the submission.

Another issue raised is that the Cybercrime Bill will criminalise innocuous activities, and various examples are provided to support this contention. We have touched on this before but, to restate it, proposed computer offences apply only to unauthorised conduct and contain appropriate fault elements to ensure they do not catch innocuous activities. There will of course be instances where the proposed computer offences apply to less serious conduct. This is unavoidable and is common to many offences—for example, the offence of theft covers the theft of a pencil, and damage includes damage to a pencil. The criminal law is such that there are prosecution decisions made all the time where the culpable but minor type offence—the trivial breach of an offence—is not prosecuted. To try to restrict the offences or to navigate your way through that ends up making it very difficult to prosecute the offences.

Many of the subcommittee's examples of the ways in which the offences would criminalise innocuous activities are quite fanciful. The suggestion that the offence of unauthorised impairment of the reliability, security or operation of data held on a computer disk could be committed by a person merely criticising flaws in the data is misconceived. The offence clearly applies only to a tangible impairment of data and would not cover the publication of information about software flaws. A person who merely points out pre-existing flaws in data does not impair that data.

The argument that the whole of the World Wide Web constitutes restricted data is erroneous. Information on the web does not become restricted data simply because an Internet service provider requires a customer to enter a username and password before using the Internet. The password is intended not to restrict access to the web but to limit use of the ISP service to legitimate customers.

The contention that the definition of 'data storage device' covers library barcodes, cassette tapes and pieces of paper ready to be scanned into a computer is also incorrect. A 'data storage device' is defined to mean a thing—for example, a disk or file server—containing, or designed to contain, data for use by a computer. Unlike disks and file servers, barcodes, tapes and pieces of paper do not contain data in a computer useable form and therefore do not fall within the definition of a data storage device. Furthermore, the offences apply only in relation to data in a removable data storage device for the time being held in a computer.

The subcommittee also suggests that the offence of possession or control of data with intent to commit a computer offence creates the 'risk that mere intent will convert harmless possession into criminally liable possession'. This statement overlooks the fact that the prosecution has to prove beyond reasonable doubt that the defendant possessed the data with the intention of committing a computer offence. In order to prove the offence the prosecution will need to produce very tangible and compelling evidence to demonstrate that the person had the requisite intention. That is the answer to that.

The Communications Law Centre submission raises concerns about the breadth of the proposed new investigative powers. As we have said before, the proposed amendments do not extend law enforcement search and seizure powers extensively but merely take into account new technology. The proposed assistance order would only require the specified persons to provide information or assistance that is reasonable and necessary to access, copy or download data and could be granted only where there are reasonable grounds to believe that evidential material is held in the computer. As noted in the explanatory memorandum, requirements to provide reasonable facilities and assistance to officers executing a search warrant are common in Commonwealth regulatory legislation. Requiring a person to provide a computer password or encryption key is the electronic equivalent of requiring a person to provide the key to a filing cabinet or combination to a safe. We have to remember, of course, that you have to have a search warrant and you have to have a magistrate agree to it. They grant that search warrant with the knowledge of what the powers include. The issuing magistrate must be satisfied, and this must be taken into account.

The power for officers to access evidential material on computers networked to those on the search premises simply clarifies the existing provision and caters for the reality of the modern electronic environment. It is so simple to just link everything out. Officers will not be able to 'hack into any computer whatsoever', but will be able to access data only where there are reasonable grounds to believe that it may contain evidential material. This is what the scope of these warrants. In view of the fact that an electronic document may not even exist on a single computer but may be drawn together from elements on different computers at a particular point in time, and the ease with which hackers can download data onto someone else's computer, it is essential that police have the power to access evidential material regardless of where it is held on a network.

There are various safeguards to protect the privacy of information which is gathered under a search warrant. Australian Federal Police officers are bound by the information privacy principles in the Privacy Act 1988 and are subject to a maximum penalty of two years imprisonment under the secrecy provisions in the Australian Federal Police Act 1979 for any improper recording or disclosure of information. The AFP have said that they will review their guidelines on recording, disclosure and storage of information in light of the new offences and investigation powers. Consultation about those guidelines is occurring with the Federal Privacy Commissioner. The vigour with which that was being pursued was quite evident immediately after the last hearing. While I do not have anything to give you today, I am very certain that those responsible for considering this legislation will require a progress report or some evidence of progress on that. As soon as we can do that we will give it to you.

We have had long discussions with the Australian Competition and Consumer Commission, but we still seem to have trouble getting the message through. I will try to get it through now.

Senator MASON—Tell us more.

Mr McDonald—I am just telling you exactly what I told them. They have suggested that the terms 'computer' and 'network' be defined. The terms 'computer' and 'network' are not defined in order to ensure that proposed computer offences can encompass changes in technology. I have said this before. This follows the approach of the existing offences in which 'computer' is not defined. If it had been defined in 1989, they would obviously be concerned at the moment about the lack of coverage, but they have been remarkably durable given the change and they would not have been durable if they had defined 'computer'. There have not been any difficulties with this approach.

The Model Criminal Code report on computer offences specifically recommended that the term ‘computer’ not be defined for those reasons. The Model Criminal Code officer committee is not a committee that comes to these conclusions without thinking it through very carefully, and there was consultation on it. At the end of the day, common understanding and evidence of what it means is the best way to approach it.

The ACCC also expressed concern that the offences would impact on legitimate activities such as port scanning, spamming—unsolicited email—and refusal by ISPs to carry certain communications traffic. Port scanning is used to scan the ports on a computer to determine the types of electronic traffic that the computer can receive or send. Port scanning does not constitute access to data and most certainly does not constitute access to restricted data and is therefore unaffected by the proposed offences. As you know, I am not the most impressive computer expert. I asked one last time and I also asked other very qualified people and they confirm that. Some parts of our department involve people with the highest qualifications in this area and, of course, there is Mr Orlowski, who was here the other week.

Spamming would only be caught by the proposed offences if the purpose of the spamming were to bring a system down.

CHAIR—Did you say spamming or scanning?

Mr McDonald—Spamming.

Senator MASON—What is spamming?

Mr McDonald—It is basically like junk mail. You open your computer up and you get an advertisement for this or that. It can be misused sometimes when people put something very misleading on it. It could say, ‘The share price for such and such a company is going to go down because they are going to make this announcement tomorrow.’ That is best dealt with by specific legislation. If it is to do with share prices, then the best thing to do is to have an offence in relation to trying to influence the security market. Some people are just advertising, and that is not criminal conduct at all. However, you could dress something up as spamming for the purposes of wrecking people’s computers or stopping them from using them. It is such a broad term that you have to look at what the harm is, what the intent is. Sure, spamming will get caught in those situations. ISPs can ensure that any refusal to carry certain electronic communications on their networks is authorised by including a statement to this effect in the terms and conditions of their standard contract. So that becomes authorised.

The submission by 2600 Australia asserts that the bill places in ‘grave danger the common law privilege against self-incrimination’ by providing for an order by a magistrate requiring a person to provide information or assistance to enable officers to access a computer. I do not think I have ever brought forward a piece of legislation here without someone saying that the right to self-incrimination is being threatened in some way or another. The point is that it does not affect the privilege against self-incrimination. The privilege arises where a person is required to produce certain documents or answer questions and entitles the person to refuse to produce those documents or answer the questions on the grounds that it would incriminate them. An ‘assistance order’ is different in that it does not require a person to produce particular data; it only requires the person to provide information necessary to enable a law enforcement officer to get access to the computer. Once they have got access to the computer, the officer still has to search for it and find it. The submission also queried paragraphs 3K(3)(a) and 3K(3)(b) of the Crimes Act. I add that I would very much like to see this numbering fixed up at some stage.

CHAIR—You are not the only one, Mr McDonald.

Mr McDonald—The drafter has not let me do it yet, but it will happen soon.

CHAIR—If I delve into this I will find the phrase ‘to avoid doubt’, won’t I?

Mr McDonald—The submission queried whether those paragraphs of the Crimes Act which I have mentioned, which give the occupier of search premises the right to be present at the processing of things taken from the premises, would be removed by the bill. The bill does not affect those provisions. The other issues raised by 2600 Australia have been addressed by the earlier bits.

Electronic Frontiers Australia criticised the application of absolute liability. I have explained before that this relates to jurisdictional elements with the Criminal Code. It requires us to be very clear about what the fault element is for each element; otherwise fault elements do apply. Because there are Commonwealth aspects to the matter, we have to provide for absolute liability, simply to reflect the way in which the law would have otherwise operated. It does not affect the key culpability of what is going on here. You have to show absolute liability and strict liability. If they are applied to a specific part of an offence, it can be quite acceptable, if the key culpability does require proof of intent and recklessness—and that is the case with all these offences.

They are the main matters that have been covered in those submissions. We will give you a full written version of it, plus we have got some more statistics to support—

CHAIR—In addition to the ones that you appended to your answers to questions on notice?

Mr McDonald—Yes. We have continued to work on that. We have got some FBI stuff. We had all these incredible figures about what it costs and so on that we touched on—

CHAIR—Are you about to identify the nature of the \$3 trillion for us?

Mr McDonald—I had a fair bit of difficulty with that.

CHAIR—The committee is having some challenges, too.

Mr McDonald—It was \$US1.6 trillion but, quite frankly, the material from the Computer Security Institute probably is more useful.

CHAIR—Would you like to table that for us?

Mr McDonald—Yes.

CHAIR—Ms Chidgey, did you wish to add anything at this stage?

Ms Chidgey—No, thank you.

CHAIR—Mr McDonald, I appreciate your clarification of a number of those issues that have been raised in submissions. But even a cursory glance at the submissions tells me that there are some consistencies between submissions from other parties, which leads me to suspect that there may be some drafting and definitional issues here and that, rather than just defending and clarifying, it is best to change and clear up these matters. For example, the department contends that the submissions that have raised the issue of telecommunications services are incorrect. But it has not been raised by one; it has been raised by several. This is obviously a point which could be clarified in the legislation. Is the department willing to look at those sorts of things?

Mr McDonald—We are always willing to look at suggestions. In relation to that, we have been talking to the Office of General Counsel—

CHAIR—Yes, I see it in your notes.

Mr McDonald—We have explained in our submission that it is connected to other legislation which relates to the constitutional authority the Commonwealth has in that area. So that is one area on which, obviously, we will be interested to hear what the committee recommends. It is one area we considered very carefully before we put the bill forward. As a department, we are yet to be persuaded that it needs to be changed. Of course, the government will be able to consider what everyone has put—including the committee and in these submissions. I might say that one of the reasons that a lot of the submissions are similar is that if you actually read the submissions you will see there is cross-referencing between them—

CHAIR—Yes, there is no question of that.

Mr McDonald—We are talking cyberliterate submitters—

CHAIR—For which the committee is very grateful.

Mr McDonald—Yes. But the fact that there might be patterns does not necessarily mean they are correct.

CHAIR—In terms of the breadth of offences, you have addressed some of the concerns. There are still some claims by individuals that people may be caught who have just been innocently involved in this process. Are you sure that it is the department's view that the bill will not have that impact?

Mr McDonald—Absolutely. A lot of the offences require proof of intention. There has been some mention in some of the submissions about recklessness. However, the test for recklessness in the code has quite a firm fault element. It is used universally for all similar serious offences where you are referring to circumstances or results of conduct. It provides:

A person is reckless with respect to a circumstance if:

he or she is aware of a substantial risk that the circumstance exists or will exist: and

having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

Then you have a similar formula for where it relates to a result. So the fault elements in this legislation are by no means easy to prove. Those with a prosecution and law enforcement perspective know very well that the offences that remain in this context are still fairly difficult offences to prove, which is the reason they want these sorts of enhancements to the provisions in relation to their powers.

CHAIR—But, for example, the Model Criminal Code provisions or suggestions required elements of intent and recklessness and a couple of points which are not transposed into this legislation.

Mr McDonald—There are no problems with that because chapter 2, section 5.6 of the Criminal Code provides that where it is not stated it does apply. What they did with that particular provision in the Model Criminal Code was to state it for the purposes of the discussion so people would understand that. But, in accordance with consistency and the way we have drafted the code, it is not necessary, so section 5.6 provides that, where it is conduct, you have to provide intention—it is a default fault element—and, where it is a circumstance or a result, then it is recklessness. So the same fault elements apply.

CHAIR—I have two other quick questions. We have had raised with us by two police services—both Queensland and New South Wales—that the 72-hour time limit in relation to the removal of a thing from premises for examination is inadequate. Was there any consultation done with the police services before that was inserted in their legislation? I see that Ms Chidgey is nodding.

Mr McDonald—The 72-hour limit goes to the limit that applied in relation to search warrants right back when we did it in 1994 and we have put it in there for consistency reasons. That was all consulted through the Gibbs committee, and it is possible to extend the 72-hour limit in appropriate circumstances.

CHAIR—How does the extension occur—by an application to the court? Can you have more than one extension?

Mr McDonald—In section 3K.

CHAIR—For which, I might also say, Mr McDonald, we are also grateful.

Mr McDonald—In subsection 3A it says:

The thing may be moved to another place for examination or processing for no longer than 72 hours.

In subsection 3B, it says:

The executing officer may apply to an issuing officer for an extension of that time if the executing officer believes on reasonable grounds that the thing cannot be examined or processed within 72 hours.

And we give them notice.

CHAIR—Can you apply for more than one extension?

Mr McDonald—I do not think that this excludes that possibility.

CHAIR—What if we use subsection 3E(8) of the Crimes Act as it exists, which allows for the issuing of successive warrants which would remove that uncertainty.

Mr McDonald—I did not say it was uncertainty.

CHAIR—That was my question, Mr McDonald. I will ask you to look at that; let's not do it now. You indicated in your earlier evidence that there might need to be some slight amendment to correct that question about whether state and territory law enforcement agencies could access materials from computers pursuant to a search warrant that was issued under state or territory legislation. Have we followed that up?

Mr McDonald—Yes, I think we should do that for abundance of clarity. The state has asked us to do it and I think that is a reasonable request. What is good about it is that it is quite specific to the situation. If the committee would like to recommend that, it would be very nice.

CHAIR—Thank you for that suggestion.

Senator McKIERNAN—I have some questions regarding the drafting of offences on the bill. Perhaps I might start with the first one that has been mentioned a couple of times this evening—absolute liability. This was not recommended by the committee, was it?

Mr McDonald—No. This is only because it is a Commonwealth piece of legislation. At the state level, the offences apply right across the board. With the Commonwealth we have, of course, a constitutional framework, which means that we have to ground our offences with respect to our jurisdiction. Prior to the code, they had never been required to prove that the person knew it was a Commonwealth computer or knew it was a Commonwealth offence as opposed to being a state offence. Like the theft and fraud bill that this committee approved last year, it has very similar offences with a similar use of absolute liability in the case of, say, a burglary. If you burgle a place and it happens to be a Commonwealth property or a Commonwealth building, under the new Commonwealth burglary offence you do not have to prove that you knew it was a Commonwealth building or Commonwealth property; you just

have to prove that you burgled. It is absolute liability in relation to the Commonwealth jurisdictional aspect.

It is the same when you cross-refer to offences. For example, robbery is an offence which involves using violence. You do not have to understand whether the violence offences are necessarily Commonwealth or state offences. We use absolute liability. I am just making it clear that you do not have to prove that aspect of it. It is part of the rigour of the Criminal Code. There might be a situation or an offence that you do have to know was a Commonwealth situation. But this is not the situation where it is appropriate because the key culpability is intentionally impairing someone's computer.

Senator McKIERNAN—I do not have the committee's report in front of me. Were they, in making their recommendations, addressing the specific and separate constitutional requirements which you have explained in regard to absolute liability? Did they take them into account when they were formulating their recommendations?

Mr McDonald—By them, do you mean the Senate committee?

Senator McKIERNAN—No, the MCC committee.

Mr McDonald—It is not an issue for the Model Criminal Code Committee because they are only looking at it from a state perspective. At a state level, they have got jurisdiction to legislate in relation to the world. They do not have the jurisdictional restrictions. I am trying to think of a state example. In really young child sex offences they use absolute liability in relation to whether you know the child is under 10. That is an example of where they have used it. It is not that they have never ever used it. In that case the child is so young that actually have to prove that they knew the person was under 10 would be ridiculous. This is something altogether different, but that particular example is a state offence where the Model Criminal Code Committee have said it is appropriate for that very specific element of the offence. Offences are made up by a variety of elements of varying importance. In this particular one, this element in relation to whether it is a Commonwealth computer or not is not important. The culpability lies in damaging the computer. If you can prove that the person intended to damage the computer and it happens to be a Commonwealth computer, this offence covers it and you do not have to prove they knew it was a Commonwealth computer. As you know, most people would not have a clue. They have great difficulty in understanding these sorts of things. You should see all the letters I get complaining about things that state governments and state law enforcement authorities have done. They write to Mr Howard to complain about these things. People do not understand the delineation between the two.

Senator McKIERNAN—Thank you, Mr McDonald. In summary on that, when I am looking at the report of the Model Criminal Code Committee, I should be interpreting that as being more orientated to offences against the state—

Mr McDonald—It is a state model.

Senator McKIERNAN—as opposed to offences against the Commonwealth?

Mr McDonald—Yes.

Senator McKIERNAN—That might put a different perspective on many questions.

Mr McDonald—Occasionally the committee will make a comment about Commonwealth law, as in the drug context where we have got incredible overlapping between the state and Commonwealth. But as member of that committee you have to make a decision about whether it is a model Commonwealth law or a model state law. The Model Criminal Code has actually been put together by state criminal law advisers as well as by us. Most of the criminal

law is of course in the state jurisdiction. It has worked very well having it as a model state law. That is why we are starting to get quite a lot of picking up of the Model Criminal Code now. More and more is happening and that is very good. In this area, at the last meeting of the Standing Committee of Attorneys-General, we have had a further step forward in that process. But being a model state law is great because they can just pick it up as it is. For us, we have got to take in our constitutional limitations. We get into things like telecommunications service and language like that for that reason.

Senator McKIERNAN—I note in the submission from Mr Taylor from Electronic Frontiers Australia that they have run into the same confusion I had on this matter. They make the criticism that the changes that have been made to the Model Criminal Code have not been justified in the explanatory memorandum of the bill.

Mr McDonald—I thought we did.

Ms Chidgey—The explanatory memorandum explains why we have applied absolute liability and refers to those elements of the offences as jurisdictional connections.

Senator McKIERNAN—I made that comment in the global rather than in the specific of absolute liability—

Mr McDonald—About what the Model Criminal Code is.

Senator McKIERNAN—I made it in the context of the broader discussion that we were having rather than just the absolute liability question.

Mr McDonald—I have to concede that we do not go into great detail about that and perhaps that is a suggestion we can follow up when—I hope—the bill is introduced in the House of Reps and make that clearer.

Senator McKIERNAN—I made that explanation pretty quickly because Mr Taylor was still in the building and I did not want to misrepresent what was contained in the submission.

Mr McDonald—Yes. When we did it for the first time in the theft and fraud bill, we spent a couple of pages explaining what we were doing, because we were very fearful that people would have thought that we were—I guess we probably should have provided a bit more explanation there, but we can fix that.

Senator McKIERNAN—I will move quickly through the rest of my questions, and maybe they have already been addressed by that earlier answer about the different emphasis contained in the MCC. I have a question about ‘data held in a computer’—which was included in the MCC as ‘data entered or copied into a computer’. This is not contained in the bill as a definition. Is there a reason for that? I am looking at 476.1.

Ms Chidgey—It was discussed with the drafters of the legislation. We agreed with them that it was so obvious that data held on a computer would include ‘data entered or copied’ that it did not add anything. Because it is an inclusive definition, what we needed to specify was something that that concept might not ordinarily occur to people as including, so that we thought it was not necessary to include the reference to ‘data entered or copied into a computer’.

Senator McKIERNAN—So it just was not thought necessary?

Mr McDonald—Sometimes with drafters it is an art form in itself; sometimes they do have suggestions for simplifying provisions. While I am very much in favour of following the Model Criminal Code as closely as possible—if it is not sacred a drafter might come up with a way of making a paragraph a little bit simpler. That has happened with this committee, I might add, and there have been occasions where the committee has made suggestions which

have been taken up. It does not concern governments in terms of compliance with the Model Criminal Code. The point of the Model Criminal Code is to try and get consistency in substance. In this case it is a suggestion by the drafter that we took up as a result of his recommendation. I had forgotten about it.

Senator McKIERNAN—The MCC definition ‘modification applied in respect to data held in a computer or a data storage device’. ‘Data storage device’ is omitted from the definition in the bill. You are coming back on other matters. If you want to come back on that one it would be fine too.

Mr McDonald—Ms Chidgey will double check that.

Senator McKIERNAN—I have got it listed as 476.2(1)d.

Mr McDonald—Can we just take some time to consider that?

Senator McKIERNAN—By all means.

Ms Chidgey—Actually I can answer that. The offences which refer to modification relate to modification of data held in a computer, and data held in a computer includes data held in a removable data storage device. So it was felt that there was no need in the definition of modification to refer both to data held in a computer and to a data storage device, because that was covered by the definition as it stands in the Commonwealth bill.

Mr McDonald—We will put it all in writing but it is another example of where, as soon as a drafter sees these model bills, they immediately try to think of a way of making them better. Essentially, if it is genuinely better, we go along with it, providing it does not change the substance. We obviously would be concerned if it changed the substance. We can specifically address that in writing as well.

Senator McKIERNAN—I think the chair mentioned this particular one earlier in the evening, but I am not so sure. I might be coming at the same matter from a different angle, but I will ask the question anyway and we will see where the response goes. It deals with 477.3, ‘Unauthorised impairment of electronic communication’. This offence contains a penalty of 10 years imprisonment. The bill does not contain or explain what an element of intention is. Why is that?

Mr McDonald—The element of intention relates to the conduct element. I have actually answered this in relation to that other question. Section 5.6 of the Criminal Code applies an intention automatically to any conduct, so there is no need to mention it.

Ms Chidgey—I might add that the explanatory memorandum explains the way that the default fault elements work in relation to the very first offence, which is 477.1, and the same principles then apply to subsequent offences.

Mr McDonald—We have got it in the explanatory memorandum this time.

Senator MASON—I will be very brief. Mr McDonald, some of the difficulties have arisen in the evidence because there is an attempt to apply traditional criminal law concepts to, in a sense, novel areas of technology or novel technological concepts. I was flipping through the legislation before and I will use as an example—the chair touched on this, as did Senator McKiernan—proposed section 478.1, ‘Unauthorised access to, or modification of, restricted data’, which is a fairly mainstream offence in this legislation. You were talking about elements of the offence before. I want to pursue that for a second. In the penultimate paragraph, on page 11, it says:

This offence will apply to a person who hacks into a computer system protected by a password or other similar security measure in order to access personal or commercial information or alter that information.

What are the elements of that offence? What do you have to do? Is it the fact that you have succeeded in hacking into a computer that comprises the principal element of that offence?

Mr McDonald—The thing about it is that the conduct—which is getting in there—is, of course, intentional. Using section 5.6, it has to be unauthorised access or modification. We have a definition of restricted data, which is where we refer to the access control system, the most likely one being passwords.

Senator MASON—Let me shortcut that. That all makes sense. I understand that. How about if you attempt to break in but you fail, which most hackers do?

Mr McDonald—The rules in relation to attempt would apply to this offence just as they would to any other offence.

Senator MASON—And the problem would be evidence?

Mr McDonald—That is right. Evidence is an interesting thing. Sometimes it is really easy, sometimes it is not. But there are general principles in section 11.1 of the code which deal with that.

Senator MASON—I understand that. What element would have to be proven to prove an attempt?

Mr McDonald—I am looking at this for you. Section 11.1 provides:

11 (1) A person who attempts to commit an offence is guilty of the offence of attempting to commit that offence and is punishable as if the offence attempted had been committed.

So you get the same penalty. It goes on:

(2) For the person to be guilty, the person's conduct must be more than merely preparatory to the commission of the offence. The question whether conduct is more than merely preparatory to the commission of the offence is one of fact.

Finally, it says:

(3) For the offence of attempting to commit an offence, intention and knowledge are fault elements in relation to each physical element of the offence attempted.

You have to have intention for an attempt.

Senator MASON—I understand that. Specifically, what is 'beyond preparatory' in an offence like this? Is it turning the computer on? You understand my question, don't you?

Mr McDonald—Yes. I think that the conduct of just turning a computer on, if it is something that happens in the morning each day, you would argue was not more than merely preparatory. On the other hand, if you went about getting into a specific computer that would be an unusual computer for you to be using and one that has got special hacking software in it or something like that then the prosecution could argue that starting that computer up and starting to access some of that stuff would be something more than merely preparatory. But you have really got to look at the facts of the particular case. Attempt is not a new concept.

Senator MASON—No, it is not. I am thinking in terms of the dynamic nature of this technology that it would be interesting.

Mr McDonald—I think the way I have explained it is a pretty good way. If I bumbled into work at 8 o'clock each morning or whatever time I happened to arrive and turn the computer on, then I think the prosecutor would have a lot of trouble saying, 'He turned it on. That was something preparatory to doing something bad with it.' On the other hand, if I went to a computer that was not one that I normally used and there were other circumstances in the way

I dealt with it, then the very same activity might be regarded as being more than merely preparatory. You have to prove that you intended to do these things too.

Senator MASON—I understand that. Finally, perhaps as the logical conclusion of this: if you are trying to hack into a computer system but it is encrypted and it is impossible to hack into, what offence might then you commit?

Mr McDonald—Attempt could be relevant there.

Senator MASON—If you attempt the impossible in computer hacking?

Mr McDonald—Yes. This parliament has accepted the Model Criminal Code position on impossibility, subsection 4, which says:

A person may be found guilty even if ... committing the offence attempted is impossible.

Senator MASON—So if it is encrypted and you cannot get into it, if you attempt you can still—

Mr McDonald—Yes, that is right, because attempt is all about what your intent is—criminal intent—and that is quite reasonable.

Senator MASON—In respect of damage, then—

Mr McDonald—I might have stepped over that thin blue line!

CHAIR—You just may have then, Mr McDonald, but we will leave that on the record.

Senator MASON—Mr Taylor was giving evidence about that before and that is why I raised it.

CHAIR—That was a very interesting question, Senator Mason.

Mr McDonald—That is where the code is a magnificent document in terms of demystifying some very old common law concepts. I was able to read straight from it what the principles are. Six years ago I would have had to quote a heap of cases.

CHAIR—I have heard the word ‘magnificent’ applied to a lot of things, but I never thought I would hear it applied to the Model Criminal Code. This job opens up new avenues every day. I have totally bemused Senator McKiernan, which I did not mean to do. Mr McDonald and Ms Chidgey, in the course of those discussions you did take a couple of relatively minor matters on notice. I had another look at subsection 3E(8), and it is about issuing successive warrants. Can you just have a look at that for us?

Mr McDonald—Yes, I will.

CHAIR—Then there is one of the issues that Senator McKiernan raised. As you appreciate, we have a relatively fast tabling date, so whenever you can assist that would be helpful. I want to thank all of the witnesses who gave evidence to the committee this evening and previously.

Committee adjourned at 7.01 p.m.