COMMONWEALTH OF AUSTRALIA

JOINT COMMITTEE

on

CORPORATIONS AND SECURITIES

Reference: Electronic capital raising and share trading

CANBERRA

Thursday, 27 November 1997

OFFICIAL HANSARD REPORT

CANBERRA

JOINT STATUTORY COMMITTEE ON CORPORATIONS AND SECURITIES

Members:

Senator Chapman (Chair)

Senator Conroy	Mrs Johnston
Senator Cooney	Mrs De-Anne Kelly
Senator Gibson	Mr Leo McLeay
Senator Murray	Mr Sinclair
	Mr Kelvin Thomson

Matter referred by the House of Representatives:

The committee is inquiring into the implications for the Corporations Law, the Australian Securities Commission and securities exchanges of global electronic capital raising and share trading with particular reference to:

(a) the availability of prescribed information in electronic form;

(b) the publication in electronic form of advice or rumours about shares;

(c) electronic share hawking;

(d) the need to recognise the changing roles and activities of participants in securities markets;

(e) determining the legal, accounting and other rules that should govern electronic capital raising and share trading, including the international legal ramifications;

(f) determining how rules might be enforced; and

(g) ensuring the security of information provided electronically and transactions conducted electronically.

WITNESSES

JOINT COMMITTEE ON CORPORATIONS AND SECURITIES

Electronic capital raising and share trading

CANBERRA

Thursday, 27 November 1997

Present

Senator Chapman (Chair)

Senator Cooney	Mrs Johnston
Senator Gibson	Mr Sinclair
	Mr Kelvin Thomson

The committee met at 10.38 a.m.

Senator Chapman took the chair.

CLIFT, Ms Jenny, Senior Government Lawyer, Information and Security Law Division, Attorney-General's Department, National Circuit, Barton, Australian Capital Territory 2600

FORD, Mr Peter Malcolm, First Assistant Secretary, Information and Security Law Division, Attorney-General's Department, National Circuit, Barton, Australian Capital Territory 2600

ORLOWSKI, Mr Stephen Robert, Special Adviser, IT Security Policy, Information and Security Law Division, Attorney-General's Department, Robert Garran Offices, National Circuit, Barton, Australian Capital Territory 2600

CHAIR—I declare open this public hearing of the Joint Statutory Committee on Corporations and Securities and welcome representatives of the Commonwealth Attorney-General's Department. This is the first in a series of hearings that the committee proposes to hold during its inquiry into electronic capital raising and share trading. This hearing is being held while both the Senate and the House of Representatives are sitting, so we may have to adjourn periodically to allow members to leave and cast their votes if divisions occur, but I hope this will not unduly disrupt proceedings.

The committee prefers to conduct its hearings in public. However, if there are any matters which you, as representatives of the department, wish to discuss in private, we can move into camera at your request.

Having made those few introductory remarks, I now invite you to make an opening statement before opening the meeting up to questions.

Mr Ford—I do not intend to make any opening statement, except to briefly introduce ourselves in a little more detail for the committee's benefit so that you understand what we are each working on and that sort of thing, which might help with the questions. I thought it would be more useful to move into questions.

I have general overview of the work of the division. In relation to our submission, I suppose I would be responsible for most of the first part going up to about paragraph 26. Jenny Clift is working on the legal aspects of electronic commerce—the framework required for it and so on. Steve Orlowski is concerned with other aspects and is working on OECD committees and so on; he also leads an APEC task force on authentication.

CHAIR—Can you tell us a little more about the work of the electronic commerce expert group that was established within the department by the Attorney-General and, in particular, what you regard as the likely outcome? Is that possible at this stage of the reports that are due in March l998?

Ms Clift—The expert group is currently working on its report. It is basically looking at two groups of aspects. The first aspect, which is mentioned in the submission, is the UNCITRAL model on electronic commerce, and its possible adoption in Australia. The UNCITRAL model deals with some fairly fundamental commercial transaction type issues, and provides some basic rules for how to deal with matters like legal requirements for signatures, record retention, contract formation and so on in an electronic environment.

The second group of issues relates to authentication, which can be split into two issues again. One is really giving legal effect to signatures, the basic issue of authentication, and the second is the legal framework required for what is described as a public key indication framework or a public key infrastructure.

The report will be finalised in March, but I cannot really give you too much clue as to what is going to be in it. The group is, in general, moved by the concern that we do not have an excessive amount of regulation, and is looking at what are the minimum requirements in order to make the transition from paper based transactions to electronic transactions without having a huge amount of legislative infrastructure put in place.

CHAIR—It seems to me that there are quite a few different groups that are looking at electronic commerce within the total bailiwick of government. As well as that group, is there not a group in Senator Alston's department that is doing some work? Within the parliament there is the Joint Committee of Public Accounts which is, I think, doing an inquiry, as well as the inquiry we are doing. Each of those groups is looking at different aspects that are relevant to their own terms of reference and areas of responsibility, but do you think there is sufficient coordination between all those different areas that are being examined to bring, if you like, a whole of government policy approach to the issues?

Mr Ford—I can probably only speak for the executive side of government, but I think the government's announcement of the establishment of the National Office of the Information Economy is intended to do just that—to draw the various strands together. We are certainly not going off on a frolic of our own. It is certainly integrated with other work going on within Senator Alston's purview relating to that committee and so on. So we will relate our work to that, and it will be brought forward for government consideration at around the same time as that committee is reporting.

CHAIR—A few weeks ago I was able to attend the International Organisation of Security Commissions conference in Taipei and one of their sessions was devoted to electronic commerce. As an adjunct to that conference, the International Bar Association ran a full day seminar on electronic commerce. It seemed to me that their main focus was actually on the domestic operation of electronic commerce rather than the international aspects of it. I got the sense that they were almost putting the international aspects in the too-hard basket and that they were focusing on the domestic aspects because whatever problems were evident there were reasonably soluble; the international aspects still seemed

to be quite difficult. I note in your submission you say:
The achievement of a globally uniform commercial legal framework will be problematical.
Again, that indicates that you are perhaps somewhat pessimistic about the international aspects.

Mr Ford—Yes, it might be helpful if Steve Orlowski outlines the work of the APEC task group, because I think that is one area where there have been promising developments.

Mr Orlowski—And the OECD, because this can work there as well. The APEC telecommunications working group has established a task group which is looking at public authentication in general. It has split it into three areas: a legal area, a technical area and a general framework administrative area. The legal area is basically going to be work that should be done by UNCITRAL, which is already well developed in that area. The technical side is seen as being done by international organisations for standardisation in that the International Telecommunications Union, the Internet Engineering Task Force and a number of standards bodies groups will look at the technical standards.

In the middle is the framework area, which is not really technical and not really legal. It is a mixture of government policy, business policy—that side of things. That has been identified as work that APEC and OECD should work on together. We have got a preliminary report that we have produced with the APEC task group, which we will be happy to pass on to you. It identifies the sorts of issues that need to be addressed, where they need to be addressed and where the different international groups need to work together to undertake that work.

That report has now been passed to the OECD. I attended an OECD conference on electronic commerce in Turku, Finland last week which was looking, again, at where the two areas could work together, and with a target of delivering a number of specific deliverables by the time OECD ministers meet in Ottawa in October next year. So not only have they identified where this sort of work needs to be done at an international level; they have also decided on some target dates in October next year. Within APEC, there are some even tighter deadlines to try to get some stuff done by July next year—but purely aimed at international inter-operability. It does not look at the domestic scene at all on this.

Mr Ford—Right. When I wrote that part of the draft, I had in mind more the debate about encryption for confidentiality purposes than authentication. On authentication, I think there are more promising signs, as Steve has just indicated.

I will just finish on the OECD side of it, unless you want to add something. There will be some work going on there early next year with the joint government private sector conference on problems of achieving inter-operability in authentication internationally. It is quite a promising sign and we, in fact, were some of the people pushing for that.

On the encryption side for confidentiality, OECD guidelines were produced and released early this year, and I have brought a copy of those, if the committee would like to have them. They deal with the problem of getting a balance on the whole encryption side, which raises law enforcement and privacy and so on.

Senator COONEY—On encryption and the international sphere, are we able to assess the ability of Australia to control that, or is it going to be controlled by overseas forces? The United States, for example—or perhaps Japan or Europe—is quite clearly going to be very powerful, and you might think its commercial law and its law on encryption are going to prevail. But, given the international nature of all this, what part will we be able to play as a nation in the law that comes to operate in this area?

Mr Ford—I agree, Senator. The way we are looking at it is that the US does have a dominant position, and US firms are in a dominant position. The US, as you no doubt know, is pursuing a policy of trying to encourage a key recovery system through its export controls mechanisms. That seems to be getting more and more tacit support from companies that are signing on for that program, and thereby getting export permits. I think we have to expect that, to a very large extent, in Australia we will be takers of the technology that we get from the US.

The other large players are the European Union and Japan. It is difficult to predict exactly where the European Union countries are heading, but it is already clear that they are not heading in exactly the same direction as the US. Japanese policy seems to be focused more on authentication, rather than giving any attention to this encryption issue. So, in Australia, we are going to be takers of technological applications from those three areas. We need to adapt our law to fit with that environment where we get the different systems competing.

At the same time, it is true to say that Australia is somewhat of a player in this area—perhaps more than one might expect, given our relative size—because the industry here is quite advanced, even though it is small. Australia is recognised as having a voice in these international things. That may be the reason why we ended up chairing this particular committee, because we were somewhat of a different party from the Europeans or the Americans.

Senator GIBSON—As of today, consumers in Australia are scared to use their credit cards over the Internet because of the security problem. Telstra has just established a new system and I understand that the other main card suppliers are about to announce or have announced systems. Would you care to make a comment giving us your views of this?

Mr Ford—The policy that the US is pushing has the attraction that it seems to offer a solution to all the concerns—the privacy concerns, the security concerns from the consumer's point of view, and law enforcement and national security concerns in terms of

monitoring attacks against the US. But it is not the only solution for security on the Internet. Some of these solutions that you have just referred to are a little different with their commercial applications—the SET protocol and so on. Even a country the size of the US is not going to determine the whole range of things. I think these things are going to evolve. Steve might like to add some more perspectives on that.

Mr Orlowski—Yes, the SET protocol, which is the Visa and Mastercard one, is a very specific protocol that only deals with credit card transactions. It is not broad enough to deal with general electronic commerce. Similarly, the Surelink—and I do not know too much about it because I have not had much of a briefing on it—is a smaller scale one.

A lot of what we are looking at internationally is a scheme which will cover both multi-million dollar transactions between banks right down to 5c per page intellectual property payment type things. We are trying to develop a scheme which is broad enough to integrate the whole lot with one framework, one set of laws and one set of technologies—albeit slightly stronger at different levels for the different transactions.

One thing I neglected to say about Turku is that as much of that conference was devoted to business as it was to government. The first day of the conference was a business run forum. The whole idea was to bring business and government together to try to work out solutions that could suit both government and business. One of the issues that came out of that forum, which is consistent with what Ms Clift was saying, is that business were calling for minimum government intervention in these sorts of areas. They wanted a minimum set of laws that are not too specific because, as the technology changes, the law cannot keep pace with it. That was one of the big outcomes out of the Turku conference.

Mr SINCLAIR—Excuse me for interrupting, but one of the things that I do not follow is that I do not know what you mean by a 'scheme'. To my mind, part of the problem is that, first, there is no certainty in any transmission. The beginning of the transmission, the middle of the transmission and the end of the transmission are all from the same source. You notice this particularly on a fax. You can get one page of a fax, the next page will slip out and then you get pages three and four. There can be all sorts of problems that occur. If you are going to introduce a scheme, how are you going to technically ensure that, from the first word to the last word of the signature or the credit card number, that message is entire. That is technical, I presume.

Mr Orlowski—Yes. It is.

Mr SINCLAIR—This is the second thing that I am not sure about with this scheme: you say that the Americans have developed a fairly reasonable proposition, but they keep on having their systems go down with viruses and hackers seem to penetrate their systems, I do not know whether it is with monotonous regularity but quite often. So that the integrity of the US systems with these schemes, which you say are working fairly

well, just does not stand up—at least as far as the public's perception is concerned.

The third thing, which is one of the real worries that I have, is that I am told that this millennium bug is totally not comprehended in most of the Asian countries. I have had advice from several fairly significant sources that, if we think what is happening to the Asian currencies now is bad, wait until the year 2000 because none of them has the knowledge or the understanding of how their machines work. Apparently, their whole computer systems—although perhaps not in Japan—are just as likely to collapse and they will be relying on machines that just do not work. So what do you mean when you talk about a scheme? How do you address those three areas, which to me as an amateur seem to be fairly fundamental problems?

Mr Ford—Could I lead off in trying to answer that and then pass to my colleagues who might have other perspectives. I do not think I can entirely answer your questions, but I will tell you what I can. On the first aspect of your question concerning the technical side, as I see it, it is a technical issue to ensure that the message you are getting at the end of your fax or electronic transmission is the same as the one at the start. If we are to construct a proposal for a legal framework which says, 'You can rely on that message as having come from me,' then we have to be sure that the technical aspects do work, if we are going to attach legal consequences to it.

Perhaps if I just address the other aspect concerning the viruses: it is certainly true that, in the US, they are subject almost every day to viruses. It does happen with monotonous regularity. The argument that I was trying to summarise on their behalf was that the proposed scheme of key recovery and so on would offer protection against this. It is not a scheme that is widely in use at the moment but, if in use, I think their argument would run well because I think the scheme would offer pretty good protection against that.

Mr SINCLAIR—Against viruses but not hackers?

Mr Ford—Against both, because it is meant to keep out hackers through ensuring the confidentiality of schemes. I am not qualified to give an opinion on the technical aspects as to whether that claim is true. But it is made by government authorities in the US and I think it is supported by our own technical authorities. I do not have any details on the millennium bug problem.

Mr Orlowski—On the first one concerning message integrity: public key cryptography is designed to protect the messages in transmission. Part of that technology—in simple terms—adds up the number of words in a message and then encrypts that total. You can then do a comparison to make sure that the message you receive has not been interfered with, that you have got the complete message.

Mr SINCLAIR—You know that you have got the same number of words, but that is all.

Mr Orlowski—No, it is actually a bit more sophisticated than that. It can tell if you have changed a letter or a digit in a transaction.

Mr SINCLAIR—I see, so you can actually verify via a technical process that you get 3,224 words and no words have been changed.

Mr Orlowski—That is right. So if you have $1 million dollars and someone tried to change it to $10 million, it would show up in the technology. There is a mathematical algorithm that allows that to happen. So that is part of the integrity.

The reason for this framework is to ensure that you can authenticate who sent the message, verify that the message has not been interfered with and the person cannot deny sending the message—the non-repudiation of the transaction. So the technology is there now, which is what public key cryptography is all about. That is why we are talking about this public key authentication framework which is to facilitate that being used internationally.

Mr SINCLAIR—And the authentication is some reciprocal message so that if I am sending a message to you saying a number of words and you read it back, how can you be sure that it is I who is sending the message and not Grant Chapman?

Mr Orlowski—You have a unique digital signature, a unique encryption key that only you have. If you claim that the message has come from you, I can go to a directory and check that you are the person who signed that message electronically.

Mr SINCLAIR—I see.

Senator GIBSON—Are they national or international directories?

Mr Orlowski—These directories probably would be maintained nationally, but would be internationally accessible.

Senator COONEY—You have said to Mr Sinclair, 'You will have your personal encryption key.' Do we in Australia have the technical knowledge and the experts to guarantee that that will happen when that is said? Somebody might say to Senator Gibson or Mr Sinclair, 'That is your key; if you use that you are not going to get the hundred million that you deal with'—they are not into the billion yet. Do we have the technical skills in Australia to say, if somebody says to you, 'This is your personal encryption key', that it can't go wrong? Do we have to rely on somebody's assurance from overseas that that is right?

Mr Orlowski—It is a mixture of both. Smart cards with some of the technology that you would embed the key with—for example, your digital signature—would probably be manufactured overseas. But Australia does have the actual capability for putting an

encryption key on and has had for a number of years. I think DSD quote us as being the fifth largest IT security manufacturing country in the world.

Senator COONEY—But when we say that we really have to rely on what we are told from overseas to a large extent.

Ms Clift—The technology is one issue, but the framework within which you use the technology really more answers your question. You have your digital signature, but you use it within a framework. You have a certificate issued by some authorised certification authority. If every level within this public key indication framework complies with some sort of standards, you as the consumer do not necessarily need to know that all of that exists.

Senator COONEY—I will just tell you my problem. When I was hacking around the magistrates court in the early days, they had breathalysers. They would say, 'Right, now you are over 0.05, and we can tell you are over 0.05 because this machine has been guaranteed.' A few years later they would say, 'This is a better machine than the one we used to have and this one really does do it' and then a few years later it was, 'This one really does do it.' That was saying the earlier ones perhaps were not too good. The way they got over that was to pass a law saying, 'We do not worry too much about the technical faults in this machine; we declare it.' No doubt that is what would happen here. But it is a bit of a worry if we have a legal system that is not really supported by the technology. That is what has been asked up and down the table.

Mr Ford—I understand the point. I was trying to make the same point myself when I was saying that we have to be sure that the technology works if we are going to attach legal consequences to it. It is one thing to do it for civil law purposes. For criminal law purposes you have to have that extra degree of assurance.

Ms Clift—The difficulty with attaching legal consequences to certain types of technology gets us into the whole discussion about technology neutrality and whether you have laws that say, 'This type of digital signature is acceptable.' Within six or 12 months, we will have moved entirely away from that digital signature into something else. We get ourselves into a cycle where we are constantly running after the technology.

If you start today to change the law from this sort of digital signature to something else, it is going to take an awful lot longer to get it through the parliamentary process. People are now talking about technology neutrality. You try to pick some objective criteria rather than say X brand is the acceptable one. You try to say that, provided that the method of authentication can provide evidence as to identity, the integrity of the message and non-repudiation of the message and perhaps some other things, then it will have this legal effect. But you do not specify technology.

Look at some of the trends in the United States. The first jurisdictions that had

legislation, like Utah, picked digital signatures and set up a framework. Moving away from that approach as jurisdictions like California, which has opted for something less regulatory. They say that a digital signature must do X, Y and Z, and has to be approved by the Secretary of State. The Secretary of State has to approve all new technologies and they have regulations. The third stage—and we have not yet seen too many jurisdictions move to the third stage—is where you try to get away from having to update anything by just relying upon some objective criteria. I am sure that will come, because you do not want to build in a three-month sunset clause on everything.

Mr SINCLAIR—That is why I asked you that third question about the millennium bug. I am told that all the systems fail. I do not pretend to understand just how it works, but it seems to me that, if you set a framework in place and everything is all right in the year 1999, but come 2000 and the 1999 calculations have failed, it does not matter what your framework is. I am told that this millennium bug is really quite fundamental. There seem to be a number of people who are spending a fortune trying to make sure it does not affect their work. How can you set up a framework to guarantee the same veracity of signal and message after the millennium bug has taken effect? Presumably, they will go through exactly the same processes and suddenly it will not be valid any longer. How do you set up a framework to cover that?

Mr Orlowski—The framework that we are talking about does not depend on the technology. The framework is how you link an individual with any particular electronic representation of them—if you like, their digital signature. Regardless of what the technology is for that digital signature, there needs to be some way of establishing that your digital signature belongs to you and not to Senator Cooney.

The framework we are talking about is that which binds an individual to some electronic means of authenticating their identity. That framework is technology neutral. At the moment, it is public key cryptography. We know there is some biometric technology starting to emerge doing the same thing which would use the same framework. The technology can change. In that way we are not completely dependent on one technology. As of this moment, there are two starting to emerge which could both work within the framework, so we are technology independent with the framework itself.

Mr SINCLAIR—And is the millennium bug not going to affect that technology?

Mr Orlowski—It should not. I cannot give a one hundred per cent guarantee.

Mr SINCLAIR—I do not generally know what it is supposed to be, but having been told these really quite extraordinary stories about it, it seemed to me there could be a flaw in any authentication procedure.

Mr Orlowski—There should not be because it is a bug within the computer and it relates to dates. When you get to the year 2000, having a double zero—which can be 1900

or 2000—means some of the computer systems are not going to be able to recognise the fact that they have jumped and that double zero is bigger than 99. In 1999 you use a representation 99. When you go to 2000, you use 00, which is less than 99, so the computers will get all confused because—

CHAIR—They will think it is 1900, instead of the year 2000.

Mr Orlowski—Yes.

Mr SINCLAIR—Although they will not know whether it is 1800.

Mr Orlowski—That is right. Instead of adding one, they will want to try to subtract 99. That will upset financial records.

Mr SINCLAIR—Will it only be in the year 2000?

Mr Orlowski—It relates to the year 2000 and any subsequent year.

Mr SINCLAIR—But then 2001 would be less than 99.

Mr Orlowski—Sorry, 001 is also smaller than 99, so you would continue to have that problem.

Mr SINCLAIR—But it does not affect all the other processes; it is only the date.

Mr Orlowski—Anything that depends on the date. If you have interest rates that depend on subtracting two dates to get your interest rate—

Mr SINCLAIR—You would do very nicely, wouldn't you?

Mr Orlowski—Yes.

Mr SINCLAIR—I must remember to tell my banker.

Mr Orlowski—That is the millennium bug. If I could come to your other question which was about the hackers and viruses, one of the objectives of this sort of scheme of using digital signatures is that they can authenticate who deals with their computers. That is a much stronger tool to keep hackers out. Instead of having a simple password which hackers can quite easily break with a dictionary, or something like that, you use these much stronger authentication techniques to ensure that only people that are entitled to access the computer in fact can access it, particularly the sensitive areas of the computer. You can put much tighter protection on who can access it and therefore have a much greater defence against the hacker. Of course, the hackers have got to be able to get in to put the viruses in as well.

But in general terms, it is recognised that we are becoming dependant on information infrastructures and that we need to take steps to protect those infrastructures themselves. I think Peter might be better versed to talk about what we are doing and what the US are doing with their presidential commission on protecting the national information infrastructure.

Mr Ford—I will outline this briefly because I am not sure if it is an area that the committee is interested in. But the Attorney mentioned the other day in a speech he gave at the security in government conference that we have written to a number of private sector bodies—basically, telecommunications, financial and some others—saying that we think there is a need to protect the national information infrastructure, to borrow a term that is originally American, and would they be interested in talking to us. A number of them have written back and said they are interested and we are about to embark on those talks.

But in carrying out that exercise, it is really an exploratory effort to exchange ideas with the private sector to see how the government and the private sector can work together to protect the whole computer environment, not just the government ones. It follows similar moves in the US and the UK.

CHAIR—I want to follow up Senator Cooney's initial question about the US dominance in the technology particularly in relation to our area of interest. Will this place us at any disadvantage in terms of our capacity to attract capital, in terms of capital raising, to attract investment, once electronic commerce becomes the dominant means of transactions?

Mr Ford—I do not think so.

CHAIR—It will not give us any competitive disadvantage or anything in that area—being dependant on their technology?

Mr Ford—I have not really thought about it and I do not know if my colleagues have any ideas. But it may give the US some advantage against the rest of the world, I suppose is the way to put it. US companies, I think, to some extent have until now been held back by the bans on exporting cryptography that meets a standard which is available from competitors of US companies. Now that that ban has been relaxed at least for a two-year period, we are starting to see American company products come onto the market. They, I think, will build up a bigger market share. They would believe that that would give them some advantage, and probably it would, against the rest of the world in attracting people. I suppose, to that extent, Australia would suffer a disadvantage, but no more than other countries.

CHAIR—You also mentioned that the European Union was going down a somewhat different path.

Mr Ford—Yes.

CHAIR—In some discussions I had with Alan Whiting of the UK Treasury, who is the person responsible for corporate supervision and regulation, he had some concerns that the regulatory path that he sensed the EU were going down was going to unduly restrict the development of electronic commerce. From a UK perspective, he saw that as a bad thing. He thought that everything should be done to encourage electronic commerce. He feared there might be some diminution of its growth as a result of the path that the EU are following in regulatory terms. Have you got any comment on that?

Mr Ford—Some European countries do seem to have embarked on a regulatory path. France, for example, has a pretty tight policy on the use of encryption. They are about the only developed country to impose controls on import and use and so on. That, I think, would be an obstacle to the international development of electronic commerce.

The British were proposing a policy, which was a very outward-looking one, which also favoured an encryption system relying on keys being held by trusted third parties. Since the change of government there has not been any announcement as to whether that is still the policy or whether a new policy is on the way, so we do not really know what is happening there.

The European Commission has put out a discussion paper which is sceptical of the American approach to key recovery and so on, but it does not really talk in terms of regulation. It is very much a market-oriented paper which would lead one to believe that, if adopted, the EU policies will be very business oriented and not have a regulatory content. So there seem to be some contrary indications. I can understand someone taking that view, but there are other indications which might lead one to the opposite conclusion.

Mr Orlowski—Certainly, in APEC and the OECD, one of the things that does have to be resolved is the European very strong regulatory approach versus Japan, North America and Australia, which is a much more market driven approach. It is probably part of the trigger of the comment that was made that there is this dichotomy between the two approaches.

Senator GIBSON—This morning I was in the public accounts committee with my other hat on, and Richard Humphry from the Stock Exchange was there with his NOIE hat on, basically saying that the cross-border transactions in the securities industry are growing so fast that the current estimate is that they are about 25 per cent of all securities trading across a national border. I think he said that only three or five years ago it was only something like three per cent. It is growing so rapidly that in fact, in the securities market, commercial trading is way ahead of the legal framework that, if you like, you are working on. He was raising the question of whether national governments are actually going to catch up with this because they are not going to have much control over this. Would you care to comment?

Mr Orlowski—I think the main objective of going to technology is neutral legislation so that you do not have to try to keep playing catch up. Yes, we might be a little bit behind at the moment, and we are trying to get that technology neutral approach that recognises the electronic business without the specifics of how it is done so that, as the technology changes, we are not going to be playing that catch-up game. If we have done it broadly enough in terms of being technology neutral, we should be able to keep up with the game.

Senator GIBSON—Back on digital signatures, do you envisage that within Australia this would be a government agency, or the government would oversee several commercial agencies as holders of such registers?

Mr Orlowski—Standards Australia produced a report on public key authentication which recommended a national root authority with a number of companies or organisations being able to operate under that, but the national root authority would be—and this is the Standards Australia approach; I am not saying it is the government approach—a company limited by guarantee made up of industry representatives, government representatives and consumer and user representatives so that it represents all interests and is, to that extent, pretty independent.

Mr Ford—Could I just add to that by saying, on your question about the legal framework, that the Attorney also said in his speech last week that he did not think what was called for was a fundamental rewrite of all our laws. It is a question of adjusting our laws and sticking with the tried and true principles and adjusting them to the new environment. I think that is the way that we are approaching the electronic commerce exercise.

Ms Clift—I would add that I think the difficulty with the increasing cross-border transactions is that it is not just cross-border between, say, Victoria and New South Wales, but it is cross-border in an international sense.

Senator GIBSON—Yes, he was using that in an international sense.

Ms Clift—The domestic law can only go so far in regulating those cross-border transactions. Probably in the majority of, say, consumer transactions on the Internet at the moment, the law that would cover those transactions would probably not be the law of Australia because people are actually buying things from the United States, and therefore Australian law really does not have the ability to control those transactions, so you end up with the consumer protections of another jurisdiction applying.

In a sense, whatever we do here will not necessarily help so there needs to be this emphasis upon international resolution. Having been involved in the work of UNCITRAL, I cannot see that that is going to happen in the next year or so because it covers so many different fronts. It is not just securities; it could be insurance, consumer transactions or just

about anything.

Mr SINCLAIR—The real question is where you adjudicate them. If it is an ordinary contract and events occur in a place where there is a contract, such as workers compensation or something, you understand that they post in the place where it is. If you sign a contract, there is also jurisdiction in a place where you sign the contract. In the areas that Senator Gibson is referring to, it will be through an electronic exchange. For example, it could be between a British company operating in America, through an Australian subsidiary for some deal in Indonesia and transferring paper accounts through half a dozen different countries.

In your legal framework, are you going to set down an understanding of the qualification you have about Australia's capacity to exercise jurisdiction? If there is a question of arbitration between the parties and you have an Australian party, wouldn't we be seeking at least to have a voice within our legal framework? An Australian company could say, 'We've been defrauded for some reason or other', because that was an electronic deal and an Australian party was involved. Or are you suggesting that it is really going to be dependent on American jurisdiction—because that would really quite worry me?

Ms Clift—It is probably just an amplification of the sorts of problems that you get in international transactions now where people do not actually deal with dispute resolution. They do not have a clause that says that in the event of a dispute, the law governing the dispute will be one thing and the site of the dispute resolution will be something else. Where people actually cover those eventualities, you do not have the same sorts of problems.

I suppose in a normal transaction, in a paper-based transaction, you perhaps have got a better idea of who you are dealing with and where they are. Electronically, you may have less of an idea of where. You may know the person you are dealing with, but you may not actually know where they are and what laws might apply to the transaction. I think people need to be much more aware of the difficulties that could potentially arise and therefore to make provision for those sorts of issues.

Mr SINCLAIR—You have canvassed that here in your paper. You talk about including:

. . . appropriate fora for the resolution of disputes arising in the course of or in consequence of an electronic commercial transaction.

That covers the area that Senator Gibson is referring to. You have not really developed that beyond recognition of the concern.

Ms Clift—No, but the concern that arises in the electronic environment is not

really all that different to the concern that arises in the paper-based environment, because for some years the Attorney-General's Department and also the International Legal Services Advisory Council, which is chaired by Sir Laurence Street, has been trying to promote arbitration as a means of dispute resolution. Attendant upon that are other concerns about trying to promote the law of Australia as the law governing the contract and trying to promote Australia as a dispute resolution centre. But it always depends upon the contracting parties agreeing that that should be the case or, in the absence of agreement, having some sort of control over the contract.

In the case of say, some sea transport documentation, the legislation actually provides that you cannot have an international arbitration and the courts of Australia have jurisdiction. Again, you can still only go so far in being prescriptive about that. You perhaps need to have a great deal of education and awareness raising with lawyers and other people who enter into contracts thinking about dispute resolution and what appropriate contract controls might be.

I suppose in the consumer context, it is somewhat more difficult. In big commercial transactions, you have usually got lawyers involved and people are aware of those things. The average consumer says, 'Hey, I want to buy a CD in the US. I don't really care about the contract. I don't even know what the contract terms are, because I press the button, the order goes through and I put my credit card on', and in 99 per cent of cases it probably does arrive in the mail box. It raises all those sorts of consumer concerns that we have dealt with through our consumer legislation about consumers being aware of the contract terms and those sorts of issues. I think the ACCC has in fact got a discussion paper out which looks at the possibility of coming up with some international codes to deal with some of those issues.

Senator COONEY—Take the example of Sir Laurence Street, if he does a mediation or an arbitration in Australia and Australia has control of it. This is what has been asked all morning. For example, if it is something to do with Africa, the United States, China or what have you, what real force do we have as a nation in settling those matters?

I will not name a nation but what if a nation says, 'We are just not interested in fulfilling the obligations; we are not particularly interested in arbitration'? Is the reality of this that we are in a pure market, that if you cannot judge the person you are dealing with, then that is your bad luck? Have we got to that point?

Ms Clift—I would still maintain that that is really an extension of the sort of circumstances you have now. There is an international framework for dealing with arbitration of contract disputes, recognition of arbitral awards from foreign jurisdictions, and what we have to make sure is that the mechanisms that are in place now for a paper based contract equally apply or can be applied in an electronic environment.

There may be some problems with the conventions because they have writing requirements or they require things to be signed, and that is obviously something that has to be addressed internationally. But I do not think there is any reason to suppose that we suddenly find ourselves in the Wild West where nothing applies, because we do actually have these mechanisms in place.

Senator COONEY—Except that you have got a lot more immediacy, haven't you? With written documents at least there is something that is real in the sense that you can make copies of it, it is put on a plane and it is sent off, and you can even have time to think about it. With electronic stuff, I would be putty in the hands of Senator Gibson; he would whip this off and say, 'I want an answer straight off,' and away I go. It just seems to me that the environment is a bit different.

I understand what you are saying. It is legitimate, as you say, to say, 'This is really just an extension of the exchange of papers. It is an exchange of electronic messages.' I cannot understand the technology at all, but it just seems to me that there is a big difference and that that additional electronic exchange does make a big difference to the way we are going to have to handle it.

Mr Orlowski—We have had telex—

Ms Clift—Telex, fax—

Mr Orlowski—and telegraph for quite a number of years and we have been able to deal with that.

Mr Ford—What you are saying, Senator, I think, is that in practical terms there is a difference because you flick on a screen and you press a button and away it goes. I think that is true. But there is not a lot that could be done about the legal principles. The answer really lies more in consumer education.

Senator COONEY—That answer seems to me to make a lot of sense.

Mrs JOHNSTON—I do not think you would ever get a 100 per cent proof system. My only concern was keeping out hackers and I think you have answered that reasonably well. I agree with you, this is really an extension of what happens at the moment. At the moment there is no real protection even in the paperwork that you have because you have to deal with so many different bodies. If you can put that into place and make it better still, you are doing a great job.

CHAIR—Could you perhaps elaborate on the constitutional issues that you allude to in relation to Australia's domestic regulation area?

Mr Ford—I guess the fundamental power is the communications one, use of the

telecommunications services and so on, which gets you some way because of the very nature of the medium that we are using—telecommunications and so on. External affairs would be relevant with some of the laws or model laws that are being drafted—the UNCITRAL model law, and so on. It is probably sufficient for the moment to focus on those two. There may be other heads of power that might become relevant when we get matters to the stage of further legislation. But if things turn out the way they appear to us at the moment, it may be more a matter of amending existing laws than putting in a sweeping new Commonwealth law on electronic communications. So a range of constitutional issues might be relevant.

Ms Clift—I will just add that, at least in the commercial sphere, the situation is that states and territories generally have legislation dealing with a number of issues such as the sale of goods. Even the Corporations Law relies upon that referral of power. If the Commonwealth, for example, were thinking of enacting electronic commerce legislation at the Commonwealth level, as Mr Ford suggested, then you would have to look at whether we can actually do that under the telecommunications power. You would have to look at whether we could go far enough to cover everything so that we ended up with a national law. With uniform law, invariably someone falls out along the way or it takes 10 years to get every jurisdiction to enact it.

CHAIR—If you were in a situation where an American company was offering shares or equities to a potential Australian investor over the Internet in such terms that were consistent with the applicable American securities regulations, is that adequate, or do they need to be subject to Australian securities regulations?

Mr Ford—If you look at it in terms of consumer protection, perhaps there is a case for some additional laws. I guess my starting point would be that we should take the American law as it is and people should operate under the law of the applicable jurisdiction. I will go back to the previous analogies. If we are doing things like that in paper form at the moment, I do not think we would expect any special protection from Australian law.

CHAIR—I suppose the issue would be if someone was purporting to be an American company issuing securities and they were not.

Mr Ford—Yes.

CHAIR—That comes back to the encryption and the key system and so on.

Mr Ford—Yes. In relation to the security aspects and law of fraud and so on, if it is an Australian company or otherwise within our jurisdiction, we could get at them that way.

CHAIR—I thank each of you for making your time available to the committee for

the hearing this morning. What you had to say has been very useful in terms of our inquiry.

Mr Ford—Thank you.

[11.33 a.m.]

ARNAUD, Ms Isabelle Marie Veronique, Project Officer, Australian Competition and Consumer Commission, 470 Northbourne Avenue, Dickson, Australian Capital Territory 2602

SPIER, Mr Hank, General Manager, Australian Competition and Consumer Commission, 470 Northbourne Avenue, Dickson, Australian Capital Territory 2602

CHAIR—I welcome Mr Hank Spier and Ms Isabelle Arnaud from the Australian Competition and Consumer Commission.

This hearing is being held while both the Senate and the House of Representatives are sitting. There may be occasions when the bells will ring and we will have to attend divisions, so that will interrupt our hearing. I hope it will not be unduly disruptive to the conduct of the hearings.

The committee understands that the ACCC is not directly involved in the regulation of electronic capital raising and share trading, which is the focus of our inquiry. However, the ACCC is a regulator with an interest in, and familiarity with, a large number of electronic commerce issues, and its experiences and strategies in this environment are of considerable interest to the committee.

I now invite you to make an opening statement, if you wish, before members of the committee ask questions.

Mr Spier—I will be fairly brief and perhaps summarise what we said in our submission with a few extra points. As you pointed out, the commission does not have a special interest in this area, although it certainly has an interest. The commission is an economy wide agency in terms of the consumer protection or the competition provision sections of the Trade Practices Act. Of course, it is soon to have a fairly substantial and important new small business area too.

The commission has long had an involvement in these types of areas, and of course electronic commerce is an updated version of things that have happened before, although far more difficult to grasp. With mail order, there has always been a similar problem in the past. The use of anonymous post office boxes and those type of things have caused some issues. There were various strategies that were undertaken which perhaps have some role here, which I can come back to later.

The commission recognises that there are significant economic benefits to be gained from the advent of electronic capital raising, share trading, and electronic commerce generally. The commission, not being a policy agency, really cannot look at what can be done in terms of law, although it can speculate and perhaps give some views.

But that is not its ultimate role.

The Trade Practices Act of course is a very well-established framework which regulates a whole lot of areas, including share trading, capital raising, and if there is any misleading conduct, any anti-competitive conduct, or related issues.

Picking up one of the things that the people from the Attorney-General's Department said, I am not as pessimistic in getting Commonwealth-state cooperation in this area, because there is a very good, I suppose, precedent in the Trade Practices Act. The Commonwealth Trade Practices Act, especially the consumer protection sections, was enacted in 1974 and, in the next six to seven years, every state parliament then enacted mirror legislation. It is a fairly successful example—in fact a dramatically successful example—of Commonwealth-state cooperation.

We now have basically the same, what is called, part V, which is the consumer protection provisions throughout Australia, so business faces the same law. There is very considerable consistency in the actual black-letter law, and in terms of administration there is very close cooperation between the regulatory agencies at the Commonwealth, state and territory levels. There is a very good precedent and of course that can certainly be built on.

The other issue, particularly in the area of electronic commerce—but not only there—is the need for international cooperation between nation based regulation agencies to promote the harmonisation of investor protection rules, exchange of information in relation to the detection and prevention of frauds, and coordinated enforcement action against unethical businesses. In that regard, in the middle of October, the ACCC coordinated an international Internet sweep day. How many agencies were there in that?

Ms Arnaud—Seventy agencies in 30 countries around the world took part in that sweep day.

Mr Spier—Seventy agencies took part in the major sweep day, looking at suspect sites, not only in the financial service area, but generally. That is a start of a longer term program. We hope to do that again and again with the same and expanded cooperation from agencies—from consumer protection agencies, and other similar agencies—in all kinds of countries, from the ones you would expect to some other countries. I think, Senator, you mentioned China and others. They are not on board yet, but some of the similar countries are. We have not yet convinced Nigeria. Of course, we all get the daily letter from some of the people in Nigeria.

That is certainly a good start. It is a small start, but it is a good start. It is something that we think needs to be built on. At both the national level and the international level, there is the opportunity to look at codes of conduct to offer us a market sensitive and practical way of improving the degree of protection and confidence

that consumers expect, without in any way straining the industry.

It may be that, as part of an education program, the consumer should only deal with those sites or, for that matter, those countries that adhere to a code of conduct and have the necessary endorsement. If the sites or the countries do not do that, then the consumer or the small business person, or whoever, needs to be very aware.

The commission has issued—we have sent you a copy—a discussion paper on global enforcement in a lot of these areas—it is not just in the financial service area; it is much broader—to try and test some of the concepts and face the fact that electronic commerce and other global issues are facing us and will become very, very major issues. As an enforcement agency, at the domestic level, we are starting to look far more into the global context, because the problems we have seen in the past at the domestic level, and which have largely been overcome, will now face us again in a much, much bigger way in the global marketplace. Thank you.

CHAIR—Thank you very much for those additional comments. In your submission you refer to the need to continue the provision of information by corporations about their activities and their securities in paper form because some groups—pensioners and superannuants—may not have the familiarity or availability of computer technology. Do you see that as an ongoing requirement?

Mr Spier—Probably not. I think it is a transitional requirement probably for a while. Think of people around who are probably still very comfortable with having documentary, actual hard copy. Over time that will change. I think we have all heard the comment about the paperless office, but it does not happen; people still seem very comfortable with paper. I think it is a transitional issue.

I suppose if you go back to the old days of—they are still going on—mail order, one of the things that was put into the mail order code of conduct is that the companies who were major mail order companies, if that was their form of business, had to have a display room in the major capital cities so that people could actually go and see the product, if need be, to try and get it. It was building up a bit of trust again that the product was there and people could go and see it; most did not go, but some could. I think it is the same sort of concept here, but it is transitional. In 50 years it will be all gone.

CHAIR—Does the fact that some people do not have familiarity with the new technology mean that it is unequal—that, even though the paper information may continue, in terms of timeliness and so on, there is potentially unequal access to information between people?

Mr Spier—Certainly; but that exists throughout the whole economy. A lot of this paper based information either is hard to get—although it is not so hard to get these days—or may be very hard to understand, particularly in some of the more complex

financial services. We have always been very concerned that there are plain English versions of everything, or that that material is easily available. Ironically, through electronic means, things are more easily available. But, as to whether people are comfortable to access it, that is still something that needs to be massaged.

CHAIR—You refer to the inevitable increase in transactions where operators have no physical presence in the consumer's jurisdiction, and you say that that raises jurisdictional impediments to nation based regulatory and enforcement agencies. You also say that deficiencies in national legislation mean that there is a need for international harmonisation of rules to enable Internet frauds committed in Australia by overseas operators to be prosecuted in the operator's jurisdiction. If we cannot get our national regulatory regime effective in this area, what chance do we have of getting an international regulatory regime effective?

Mr Spier—I am not sure whether we do all that badly at the national level—clearly it is not perfect. But I think we need to try and do something at the international level. In some areas, for instance, in the competition area—the so-called antitrust area—we are entering into treaties with enforcement agencies in other countries. They will act on our behalf and we will act on their behalf, because of those jurisdictional problems.

In many cases under the Trade Practices Act we have far more jurisdiction than people think. The A-G's people were talking mainly about the law of contract. I think Mr Sinclair picked up the right point about where we do have jurisdiction. If someone globally aims a misleading advertisement at Australia and someone in Australia picks it up that is a potential breach. However, if there is no-one in the jurisdiction you can take action against, then it is a theoretical breach. If they are in the jurisdiction, and if they do have a branch or agent here, you can take action. It is getting hold of people that is the difficult bit. But if you enter into treaties or arrangements with other countries, you can certainly do it, even where that is not an offence in that particular country.

Senator GIBSON—Going back to your international search for wrongdoers last month, what did you find out?

Mr Spier—We will publish the result—in fact, Minister Truss will announce the outcome—but we found a significant number of what we would call suspect sites based on our own experience and other people's experience. The bulk of the business is very honest and very ethical but there were a significant number of suspect sites.

CHAIR—This is from the sweep you did?

Mr Spier—Yes.

CHAIR—Are you able to tell us how you went about it or is that revealing secrets?

Mr Spier—Yes. You are one of the ones in front of the terminal.

Ms Arnaud—On a specific day, which was decided ahead, but not disclosed to the public, all those agencies involved in the sweep, logged into the Internet on that day and surfed the Net looking for get rich quick schemes such as pyramid selling, investment opportunities and schemes where people were asked to give $50 or $100 to get huge returns, which of course never arrive.

Mr Spier—Except for them!

Ms Arnaud—Those sites which we thought were a bit of a problem were sent an educational message which said that we believed that they were in contravention of the fair trading laws of their countries. More recently, about a week ago, we did a follow-up sweep day looking for the same sites to see whether they had changed the way they operate or whether they had closed. Those who have not close will be forwarded to the agency of the country where they are based for some further action.

Senator GIBSON—Did you find any suspects in Australian sites?

Ms Arnaud—Yes. We had some in Australia and a lot overseas. A lot of things which come to Australia are based overseas.

Mr Spier—The newspapers here have a code of conduct which they worked out with us but it occurs in some of the publications you pick up. I can show you about 10 or 12 so-called suspect sites in the papers. It still happens here but we do regular sweeps to have a look at that area. If we can enhance that international cooperation, which we got, and we were very surprised at the level of cooperation, it is a good start. Whether that can keep going or whether other things happen, we just do not know but we are going to keep pushing it.

CHAIR—Do you see a problem with the possibility of companies playing off one jurisdiction against another and physically locating in countries with the lowest regulatory regime?

Mr Spier—Of course. I suspect most people in this room have had the letters from Nigeria. For years unsolicited directory entries have come from Liechtenstein. They initially came from Germany, then they came from Liechtenstein and then they came from all kinds of other places. When they were coming from Germany, the German authorities closed down their postal box, because that was the way they were operating, but then they moved it to Liechtenstein and they are still there. They send out bills for $500 or $800. There are warnings in the press about them. The old ships of convenience concept can happen in this area, too. So countries need to make sure that it does not happen in their country. If there are some countries that are not prepared to address it, we should try to isolate them or educate them. With the Liechtenstein thing, I am sure it makes a lot of

money for the Liechtenstein postal service. However, it is getting very well known and people are now fully aware of it because even in the blurbs we put out we say, 'If it has a Liechtenstein postmark, be a bit concerned.' It may be legit but it may not be too. International treaties and international cooperation will hopefully overcome some of that, but it will never overcome it totally.

Senator GIBSON—I am not too sure whether you were here when we were discussing with the A-G's people digital signatures and registers of—

Mr Spier—No, I was not here for that.

Senator GIBSON—They were saying that they were working on a plan for authentication, a register of digital signatures. Telstra has announced Surelink, and Visa and other companies are bringing out similar schemes. Do you have any concern about these processes?

Mr Spier—There is a privacy concern, which is not our direct concern. I suppose it depends on how well it works. As an agency, we have had concern about something that is slightly linked. If a business takes a reputable credit card, that gives them an aura of authenticity even though most of the companies do not really check those types of issues. If the credit card companies also develop this system of digital signatures and all that, it adds to this belief that what is happening is okay. There needs to be some protection, generally, but any safeguard is better than none. They are not perfect. I do not know whether they can be hacked or God knows what.

Senator GIBSON—If people are defrauded via electronic commerce, would you expect that you would be one of the first ports of call for people to complain to? In other words, can you act as an agency for informing the community about what is going on?

Mr Spier—Certainly. Obviously, we share the consumer protection jurisdiction with the states and territories. There is a fairly clear working relationship as to who does what so that we do not trip over each other. But, in the electronic commerce area, they are basically going to leave it to us, or to anything the Commonwealth government might do, because of their concern that states cannot do that by themselves. We get most of the overseas based complaints. The various state agencies would pass them onto us.

We have done in the past, and we still do, a lot of information work going back to the old directories, for instance, the Liechtenstein one. A couple of times we got Telstra to put notices in every one of their bills saying, 'If you get these kinds of bills, be careful'. We see ourselves as having a fairly major role in this area, and we are probably best placed to do it too.

Senator GIBSON—Are you getting many complaints now about electronic commerce transactions?

Ms Arnaud—It is increasing. We are getting a fair number of complaints, especially with the publicity given to the sweep day.

Mr Spier—We got a lot after that. It will no doubt grow. I noticed an article in this morning's *Financial Review* on page 43 which said that a lot of people are buying books and CDs on the Internet, and that is increasing dramatically.

Senator COONEY—Was it a Christmas tribute to your chairman?

Mr Spier—No, but we were before another committee last week and he made that very point, that increasingly people are buying CDs offshore. Anyway, that is another issue.

You can see that it will increase. Australia has one of the highest levels of access to the Internet at the household level in the world. Just go into our office, every staff member in our place has got access to the Internet. I am not suggesting that they would be using it for any private purchases, but the psychology, the culture, is now access to things like that.

Mr KELVIN THOMSON—Your submission referred to the direct marketing code and you said that could serve as a precedent for looking at electronic capital raising and share trading. Can you tell us a bit about how the direct marketing code operates?

Mr Spier—It operates still on a voluntary basis; that is its main weakness—distance selling operators which are mail order or telemarketing companies, or anyone who does not deal with people face to face. It is based on the old mail order code and other codes that have been around for a long time. There are disclosure requirements; there are all sorts of things that go wrong; there is how things are refunded. It is a fairly detailed code that has been worked out for the last three or four years between all the state, territory and Commonwealth consumer protection agencies and the industry. The code has been accepted by the industry, or at least by most players, but it is not mandatory. That is the main weakness in any code like that: not everyone must abide by it. I think it certainly is a very good start if Internet sites are prepared to abide by the code, but it is not enforceable.

Mr KELVIN THOMSON—That is the problem, isn't it? In the nature of things it is the very ones that you would be most concerned about who would not be interested in observing a voluntary code.

Mr Spier—No. But if you do have a system that says that this particular site abides by the code—of course, they can lie about that too—that is when I think there should be very swift action by any regulator to stop those kinds of claims. You would almost have to have an international agreement where they would do that: where it is basically a false statement if they do not abide by the code, and they are not accredited.

There should be a very swift way of acting against those people. If they abide by the code they can say so, and that gives the consumer a certain level of comfort. It is not total comfort, but nothing is total comfort.

The direct marketing code is a long time coming I would say. All these codes are. But it is one that is workable. There is now a precedent in some of these areas. If it is felt to be of such value and importance, maybe a code of that nature could be made mandatory. Under the small businesses package that the government has recently announced, the franchising code will be made mandatory and the oil code will be made mandatory under the Trade Practices Act.

CHAIR—When they eventually get the oil code.

Mr Spier—It is getting there. The oil code exists. It is the new improved oil code that is going to be mandatory. It will get there.

Senator COONEY—If you could make pure the international trade that goes on the Internet, what difference would that make to your decisions about issues like mergers, takeovers, competition and things like that? Would you start saying, 'This system is all purified now and we have got to look at it in terms of what competition is around the globe'?

Mr Spier—It is not so much whether it is purified, although I suppose that is one way of looking at it. In any merger you would now ask, 'All right, these two domestic companies are merging, but does that substantially lessen the competition?' One of the main factors in that always is, 'What is coming in in terms of imports?' and the Internet is another form of import.

Let us take the old favourite of CDs again. Let us say that two record companies here were merging and, on the face of it, it looked like that would substantially lessen competition in the Australian market—there is no external market. But if there were a significant flow into Australia through Internet commerce in CDs, that would provide the discipline upon the Australian merged entity in terms of the competitive market.So we may say that what in a theoretical sense looks like a substantial collusion actually is not. That happens with a whole lot of markets. For instance, there are significant imports of whitegoods. When you look at a whitegoods merger, imports are the very first thing you look at.

Senator COONEY—Do you make an assessment of how safe it is to trade on the Internet, say in whitegoods?

Mr Spier—You make a judgment, and it has to be a judgment as to whether that level of imports is realistic and sustainable. If it is a black market, for instance, then you might say, 'That might be stopped.' But if it is legitimate, normal, commercial—and we

will not make a moral judgment, but we have to make a judgment whether it is sustainable; it may be that it is not too legit, but it is never going to be stopped—there is the law. That is a factor, and you take that into account.

Senator COONEY—Your organisation and you yourself obviously are very conscious of the need to purify, which is a word I could use—to have a legitimate exchange.

Mr Spier—Of course.

Senator COONEY—It seems to me, to get it working well around the world, every other nation and organisation like yours has got to get that same sort of sense. Would you care to make an assessment of how far that has gone?

Mr Spier—The sweep that we did, which I know was a very small start, was 70 agencies around the world. That is not a bad start. I think the will is there. We looked mainly at the small end. You are looking at frauds that are obvious on the Internet and other things like that which you can see on the face of it. It is quasi consumer, quasi small business. Once you get into the big end of town, I am not sure whether the same will is there because it is left almost to, 'Well, they can look after themselves.'

Senator COONEY—I was just thinking within Australia you are a regulatory body, but clearly you have got, I might say, over the years, a good relationship with other regulatory bodies.

Mr Spier—We have very good relationships with many of the overseas agencies. But it varies, and in some—

Senator COONEY—But if you do get that, I as a consumer can feel a lot more comfortable, I know that.

Mr Spier—We are certainly strongly pushing the international issue. I think lots of countries are too. There has, for a long time, been an international network loosely based on the OECD membership—but not only the OECD membership—where we exchange information and we help each other in terms of closing down, say, businesses or doing something where we can if things are happening in one jurisdiction—if someone is sending bogus lotteries from Australia, Canada or vice-versa. It is all small stuff, but again, it is a start. There is extensive cooperation, but there are always a few problems. There were problems with some countries' laws in terms of disclosure information that caused a few problems. Some countries do not allow disclosure to aliens, which means anyone who is not from their country. So there are still some things to come over.

But the sweep was a very good start, although there is not an exchange, necessarily. There is some exchange of information, but it is not on a permanent basis,

and it is not that dramatic. But, say, with Canada, the US, New Zealand, Malaysia, Japan—although they have problems in terms of what they can tell people—the UK and Europe, there are very close relationships with lots of those areas in the anti-trust area, which has also merged into the consumer area. You tend to have cross-linkages. I think it is going extremely well, but slowly.

Senator COONEY—But, following on from what you say, the picture you have given me is that if you can get a group of countries that do it and do it well, and it succeeds, I suppose it becomes a bit like the European Union itself—other people then want to join it.

Mr Spier—If you can start with a group of the ones which are part of the network which has been going for a long time—and it is often the big economies, which includes the US and most of Europe—that would be a great start. Now you still have the jurisdictions of convenience. Perhaps it is then up to that group to try and either bring them into the fold or isolate them.

Senator COONEY—If they want to get into the fold they obviously have to reform themselves, so that group itself is a big discipline on those outside.

Mr Spier—That is right. There is an issue with very small countries who act as countries of convenience because they will never be targeted because they are so small. I remember when I was working in Canada at some stage when this sort of issue came up, there was all this stuff going from the US to Europe and the US was saying that it was pretty terrible and there were all these bogus invoices. But then someone from Europe started sending into the US, and the US suddenly got concerned. But, because both markets are worth targeting, they worked very closely together—they closed down post office boxes.

There are mechanisms, but those mechanisms are getting a bit harder. Before, the mechanisms were post office boxes, the banking system. The finance system was a way to check things; that is the way money laundering is checked. Now, what you are really left with as a trigger point is the telecommunications system. That is really what you are looking at to have a point of attacking these issues or of getting hold of them because often they do not go through the banking system any more.

CHAIR—The Trade Practices Act defines a market as a market in Australia.

Mr Spier—That is in terms of competition law.

CHAIR—Not in terms of fraud.

Mr Spier—No. But still it has to happen here or to someone here. This is something that actually happened years ago. Let us say all the airlines go through

Singapore and fix the price of air tickets from London to Australia, but they are in Singapore: that is still a breach of our law because it affects the Australian market. Whether we can reach those airlines is another issue if they are not based here, but, as they are flying here, they are probably based here. So there is extraterritorial reach to some degree. Whether you can actually do it is a practical issue.

CHAIR—I have covered my area.

Senator COONEY—That was a good session. Both have been good sessions, if I might say so.

Mr Spier—Thank you, senators.

CHAIR—I thank both of you for appearing before the committee and cooperating. The answers you have given to questions have been most informative in terms of our inquiry.

Committee adjourned at 12.07 p.m.