COMMONWEALTH OF AUSTRALIA

on

JOINT COMMITTEE

THE NATIONAL CRIME AUTHORITY

Reference: Law enforcement implications of electronic commerce

CANBERRA

Monday, 24 March 1997

OFFICIAL HANSARD REPORT

CANBERRA

WITNESSES

GRABOSKY, Dr Peter, Director of Research, Australian Institute of Criminology, GPO Box 2944, Canberra, Australian Capital Territory . . . 4

MONTANO, Ms Elizabeth, Director, Australian Transaction Reports and Analysis Centre, Tower A, Level 12, Zenith Centre, McIntosh Street, Chatswood, New South Wales 2067 4

WAHLERT, Mr Glenn, Senior Analyst, Office of Strategic Crime Assessments, Locked Bag 23, PO Kingston, Australian Capital Territory 4

JOINT COMMITTEE ON THE NATIONAL CRIME AUTHORITY

Law enforcement implications of electronic commerce

CANBERRA

Monday, 24 March 1997

Present

Mr Bradford (Chair)

Senator Ferris
Senator Gibbs
Mr Filing
Mr Sercombe
Mr Truss
Mrs West

The committee met at 8.45 a.m.

Mr Bradford took the chair.

CHAIR—I declare open this public hearing of the Parliamentary Joint Committee on the National Crime Authority. Section 55 of the act which established the NCA places on this committee a duty to examine trends and changes in criminal activities, practices and methods.

Today's hearing is to enable the committee to gain a comprehensive understanding of the criminal opportunities provided by the latest electronic commerce technologies. Even if it is beyond us today to determine the proper law enforcement response, at least we and the general community will have had the opportunity to gain a thorough appreciation of the issues. I would like to underline that point, because this is such an important area that this committee needs to be well-informed on those issues if it is to do its job effectively. The committee has demonstrated its high level commitment to that cause.

GRABOSKY, Dr Peter, Director of Research, Australian Institute of Criminology, GPO Box 2944, Canberra, Australian Capital Territory

MONTANO, Ms Elizabeth, Director, Australian Transaction Reports and Analysis Centre, Tower A, Level 12, Zenith Centre, McIntosh Street, Chatswood, New South Wales 2067

WAHLERT, Mr Glenn, Senior Analyst, Office of Strategic Crime Assessments, Locked Bag 23, PO Kingston, Australian Capital Territory

CHAIR—I welcome our panel of experts. The committee hopes that, as much as possible, this briefing will be held in public. It may be necessary to have a private session at the conclusion of the public session, although I am not necessarily foreshadowing that. I understand that your report from the Electronic Commerce Task Force has now been made public, so that may enable us to refer directly to the contents of that report in public session which should be very helpful.

You have been asked to speak for a few minutes, although you can speak for as long as you want to—but I do not propose that we should go beyond 10.30 a.m. It will be important that your remarks go on the record and that all members of the committee have the benefit of subsequently reading what transpired and being fully informed. It might be best if Ms Montano could speak first, followed by Mr Wahlert and then Dr Grabosky. As the witnesses are public officials, the committee understands that you will not step over the line and comment on government policy directly, but we would certainly appreciate your help in identifying policy options that you can perhaps canvass in general terms.

We appreciate the fact that you have given us your time this morning, as you are very important and busy people. Thank you very much for that. As I have said, it is an important issue that this committee needs to be informed about so that it can carry out its role effectively in oversighting the NCA. Ms Montano, I will hand over to you first to make some opening remarks.

Ms Montano—Thank you. I appreciate the opportunity to brief you because this is an issue which Austrac is very concerned about. Austrac is both a regulator and a law enforcement agency, and therefore can probably give you a perspective on the role that a regulator can play in relation to an effective law enforcement environment. We think there is great interaction between the two spheres of government.

Appropriate regulation can provide very valuable assistance to law enforcement. It can be used to foster systems and environments which are hostile to crime. For example, it can foster the creation of systems and industry practices which try to limit the opportunity for crime in the first place by encouraging sensible defences against computer hacking and providing systems in relation to the way in which financial transactions are conducted, as is the case with the Financial Transaction Reports Act. When crime does occur, it can

make it easier to find and prosecute the offenders. Again, the FTR Act has a role to play in that; similar legislation, the Corporations Law, has both a regulatory and a law enforcement perspective.

This issue is very interesting for regulators because it shows a very big turning point in the role of regulators in a society. Historically, regulation was fairly simple and, probably because life was simpler, traditional regulators had lots of advantages over present day regulators: they knew the environment they were working in; they understood the technologies because they were relatively simple and most people understood the way in which their societies worked; they understood how criminals committed crime; they were able to identify people fairly easily as to who would be committing crimes; they were able to exercise, in most cases, exclusive jurisdiction over criminals because of the geographic factors; they could regulate slowly and incrementally and they could keep a fairly close watch on the unintended consequences of what they were doing; they could realise pretty soon in the game when the regulation tactics they were using were not working; and they were able to build on the way in which it had always been done before. So analogy was a very useful tool and it still is.

If you look at the last 150 years or so, you will see the enormous growth in the complexity of life and, particularly due to science and technology, that regulators have had to become a bit more imaginative in the ways in which they deal with the issues as have law-makers. The age we are entering now of course is not a new one. Electronic commerce as such has been around for a while. I suppose the moment you start to put all your financial records on computers you can describe yourself as being in the electronic commerce age.

But what we are getting now is a new phase in that age where we have got mass penetration of markets by systems which will change the way people conduct their activities, particularly financial transactions. It will also mean that the players are going to change. We can see that certain intermediaries are going to lose significance, and the emphasis that regulators used to place on seeking to work closely with certain strategic points along the way in a process are going to have to change. So, instead of looking to financial institutions to provide a lot of the points at which regulation could intervene, we are going to have to find some different strategies.

Traditional regulation has been challenged because the assumptions underlying the way in which business activity took place have been challenged. The technologies are developing very quickly. The combinations of technologies can make something which, on its own, has certain characteristics all of a sudden have lots of different possibilities simply because of its inter-operability with another technology. The classic case for that would be, for example, a stored value card and the ability to transmit the information, perhaps the monetary value represented on a stored value card, through to the Internet via a telephone which takes a swipe from a stored value card. It is very simply but quite a powerful example.

Regulators are going to have to look to specialised knowledge as to how the technologies work—something that in the past was not necessarily a great requirement. The reaches of the technologies mean that there are some very interesting challenges to jurisdiction, both in respect of law and enforcement. We are going to have to see more situations where there are going to be international treaties and arrangements in relation to not only the laws but how they are then enforced.

In our Electronic Commerce Task Force report we have drawn the analogy with the law of the high seas where we take the view that this is an area which geographic boundaries would indicate does not really fit into any particular niche. Agreements are reached and there are then certain presumptions made in relation to conduct so that someone somewhere does have jurisdiction and does have the power to enforce.

All the existing strategies are going to have to be re-examined to see whether they still hit the mark. It may well be that the traditional way of reporting and the traditional way that regulation will set out the machinery by which an objective is to be achieved will have to be changed.

What we see happening is that there will have to be a combination of strategies developed over time. We will still be able to develop by analogy in many cases because a lot of the developments, particularly the ones that have been happening in the last few years, really are not changes in the core features of a financial transaction. It has been the communication methods that have changed. So once we get back to the basics of the transactions, perhaps we can just make minor changes to existing systems.

There will be the categories which totally blow out of the water the way in which we regulate today and that is where we are going to have to find new strategies. We are going to have to develop strategies whereby government is more of a facilitator than a prescriber of detail, where there will be very close and strong partnerships with industry, where government will say, 'We need a capacity to do a certain thing for good government but we cannot tell you how to do that because we may inadvertently affect the way in which your markets and your technologies develop. We do not want to do that. We may well fetter your imagination rather than foster it. Therefore, we will leave it to you, the market, to determine how to actually do this. But be aware that government has certain objectives that it needs to see achieved.'

We think that perhaps there is going to be a greater role for co-regulation between markets and government where, for example, we have got phenomena arising such as Internet user associations and Internet service provider groups who are establishing codes of practice. They are trying very hard to perform a self-regulatory role. It may be that an appropriate model is a co-regulatory one where they have market regulatory pressures they can bring to bear as a self-regulatory group, but they may well need the assistance of government to give further backup to that. We think there is going to be a range of strategies and it is a question of working very closely with industry to achieve

that.

CHAIR—Thank you. Mr Wahlert, would you like to make some remarks as well? I am sure about 100 questions have arisen already but I think if we just push on with the opening statements and then we will come back to some questions.

Mr Wahlert—Mr Chairman, ladies and gentlemen, good morning. I presented a paper to the secretariat late last week. With your concurrence and in the interests of brevity, I do not intend to simply read that paper but rather to—

CHAIR—Thank you for that, incidentally. This will form part of your evidence today, so that is very helpful. Is it the wish of the committee that the document be incorporated in the transcript of evidence? There being no objection, it is so ordered.

The document read as follows—

Mr Wahlert—As I say, all I intend to do is to highlight what we think are some of the key issues that you may wish to consider in more detail at some point. I would preface my remarks, however, by saying that I do not appear before you this morning as an oracle as none of us can predict the future. The implications contained in this document evolved out of a set of scenarios developed by the Office of Strategic Crime Assessment. These scenarios were developed in close consultation with a number of industry groups and other government departments. Some of the scenarios were what you might call worst-case scenarios but I am sure you would appreciate that, in order to best protect the interests of the Australian public, Australian law enforcement needs to be prepared for a wide spectrum of such possibilities—from the best to the worse possible case. It is hoped, therefore, that the scenarios are not seen as alarmist or the works of techno-Luddites but rather as a prudent, if not cautious, consideration of some of the major issues coming out of the evolving world of electronic commerce.

I have broken down electronic commerce into what I think is probably some of its important component parts—the building blocks if you like, the supporting technologies and systems that are allowing electronic commerce to flourish. The first, and what would appear a focus of your hearing, is that of cyber payments—a colloquial term used to describe the emerging payment systems such as smart cards, transactions over the Internet, et cetera. On page 2, I have detailed some key law enforcement concerns. I am happy to take questions on them later rather than spend time and detail on them now.

One of the other key issues is that of networks or the expanding area of private and public networks such as the Internet. One of our main concerns is the increasing societal dependence, which, together with the escalating sophistication of this technology, is creating some principal challenges for law enforcement and will continue to do so over the next five years.

Probably the bottom line for law enforcement, and one of our principal concerns, is that these technologies are enabling, and may continue to enable, a surreptitious, remote and anonymous nature of offences over networks. This has particular difficulties for law enforcement, difficulties in the detection and identification of the perpetrator, which are often resource intensive and sometimes, to put it quite bluntly, almost impossible. There are a number of other key technologies that I will not go into, but they are mentioned, such as the encryption issue and digital signatures. I am sure there are some others that you may wish to discuss.

The issue of regulation was covered very well by Ms Montano, so I do not intend to go into it here. What Ms Montano said highlights the law enforcement dilemma, and no doubt it is very similar for government: how do we ensure and encourage innovation while addressing the issues required in the public interest.

Australian law enforcement is monitoring, and will continue to monitor very closely, developments in the emerging world of electronic commerce and will do its

utmost to minimise the abuses of those systems and, in particular, the ability of criminal elements to operate in these new environments. I will leave it there. Thank you.

CHAIR—Thank you. Peter, would you like to make some opening remarks as well?

Dr Grabosky—Thank you. Mr Chairman, ladies and gentlemen, the work that I am discussing this morning is based on research for a book that my colleagues Russell Smith and Paul Wright and I have undertaken over the past year. The scope of our inquiry is summarised in the document that we have here entitled *Crime and telecommunications*. I have, in addition, a couple of other papers that deal with specific aspects of this that I will leave with you this morning.

Basically, the new technologies that we are discussing provide tremendous opportunities of a commercial nature, a creative nature and a cultural nature, but at the same time they pose very substantial risks. Each of the chapters of our forthcoming book outlines a particular generic form of illegality involving telecommunication systems as the instruments and/or the targets of criminal activity. These represent the array of risks that we envisage. The policy challenge is to maximise the positive potential from these emerging technologies—the commercial advantages that Australia can reap—while at the same time minimising the downside risks.

In light of this, it is important to recognise that the capacity of governments today is not infinite. There are limits to what governments alone can achieve. To the extent that governmental activity is going to be directed at reducing the downside aspects of the new technologies, as Ms Montano suggested, this will entail a combination of activities, in addition to conventional law enforcement and regulatory solutions, to embrace certain market based solutions as well as elements of self-help. It is important that one be aware of the risks of over-regulation and that intrusive or coercive solutions may themselves have downside and counterproductive consequences that can limit the realisation of some of the great potentials that exist in these new technologies.

Let me refer briefly to a couple of the dilemmas that policy makers will confront in addressing the new technology and its upsides and downsides. Basically, the interest of the individual, balanced against the interests of the state, the choice between privacy and accountability, is something that has to be grappled with. The maintenance of a healthy democratic society and a flourishing economy requires a degree of privacy. Moreover, developments in information technology permit the tracing and matching of identities and transactions to an extent heretofore unprecedented.

On the issues surrounding the globalisation of new technology, as Ms Montano alluded to, again I would like to emphasise that it has been terribly important. The assertion of national sovereignty can be very difficult in cyberspace, a world without borders. Just to give some indication as to the difficulties here: the communications

perceived as gravely threatening by one nation might be encouraged by others. What is offensive in some states may be regarded as benign in others. Achieving international consensus that would allow us to establish the equivalent of the law of the sea is going to be very difficult, given these very profound differences from place to place in what people value.

I will speak briefly to some of the uses of telecommunications in furtherance of organised crime. In addition to the use of telecommunications facilities in the coordination of small scale crime—that is, it makes it as easy to order drugs as it does pizza—there are certain aspects of larger scale criminal activity which are enhanced by telecommunications. It has been suggested, for example, that the Cali drug cartel uses satellite communications for global positioning.

Operations of a large scale can be made more efficient, whether they be licit operations or illicit operations. It was suggested that the technological competence of the Cali cartel in 1995 was comparable to that of the KGB at the time of the Soviet Union's collapse just six years earlier. So there are some very sophisticated technologies that are available to people who would do wrong.

Technologies can also be used to obstruct criminal investigations and other law enforcement activities—for example, small transmitters which may be concealed in a consignment of contraband and set to emit a transmission in the event the shipment has been intercepted. Cellular cloning enables criminals to communicate by using a series of phone numbers unconnected to one's identity and thereby avoids systematic monitoring, if not detection.

One of the most significant technological developments of the past decade has been the growing public accessibility of cryptography—the ability to scramble communications and encode them. Encryption technology is a boon to some criminals. At the same time, encryption technology is a boon to legitimate commercial activity for the purposes of concealing sensitive commercial information in the course of normal legitimate business.

In 1996, a panel convened by the National Research Council in the United States concluded that non-government use of cryptography was increasing around the world and it had become difficult for governments to control. It concluded that not only is widespread non-government use inevitable, but that cryptography was soon likely to become an integral feature of standard telecommunications services. So this gives some indication as to the benefits and risks of emerging technologies. I will leave it at that and would be happy to answer any questions you might have.

CHAIR—Thank you very much, Peter. My marketing mind went into full gear when you were talking about the pizza industry. The aggressive nature of pizza delivery where I live is such that I can just see it now—dial-a-deal becoming a very prominent business! The analogy, I think, is a good one.

However, on a more serious note, Ms Montano's report is now a public document, so perhaps there are one or two areas that have arisen there. You have advocated the importance of a whole of government approach to policy making. Bear in mind that I am speaking for myself, anyway, in saying that my understanding of all of this is fairly limited. Crime in cyberspace is still sinking in, for me. My kids are spending all their time playing on the computer, and I hardly know how to turn it on. Perhaps you could add a little to that. Also, you have indicated in your report the various powers of the authorities that are available. Are they adequate? You talked about the issue of regulation, but I guess our concern is particularly for the NCA and whether its powers are adequate to deal with the incredible challenges that you are talking about.

Ms Montano—The reason we emphasised the whole of government approach was that one of the first things we had to do as a group was to work out what had been done before and to see what leverage we could play off that, in a fairly time limited project. What we found very quickly was that there had been enormous numbers of studies and works undertaken, both in Australia and overseas, but they almost all focused on particular areas of government or particular areas of the market, whether they be government or private sector research works.

We came to the view that, when you looked at this issue and you looked at the way in which the various parts of a society were going to be intertwined in relation to electronic commerce, the very traditional ways of compartmentalising government consideration of the issues were not going to work. We are changing the basic rules. For example, fifty years ago, Australia Post ran the telephones and the mail. Then we had a divergence, with Telecom being created. It looks after telephones, and Australia Post looks after mail.

The more these bodies explore the technology, along with the markets that they relate too, the more you will see them entering into worlds and fields that they were never historically in. For example, you are going to end up with Telstra being in partnerships with industry in relation to things like delivery into the home of a number of on-line services. So you go from telephones to entertainment, to home banking, to a whole range of things that you will be able to do via the one set of fibre optic cables. All of a sudden, in terms of government's interest in what that entity is doing, it goes outside a pure telecommunications area and goes into a whole range of things, including the financial services field.

When we looked at the work that was being done and the issues that we were interested in from a law enforcement perspective, we found that exactly the same issues that I was looking at as a regulator were what I would be thinking about, if I were back in private practice as a lawyer, in relation to my customers' and my clients' business needs. With all the issues that we had to look at, we were not the only people who had an interest in them. We were concerned to make the point that, when policy is developed and when a legislative program is enacted, some really quite careful coordination needs to be done in relation to making sure that, when one particular area is fixed up, as it were, other

areas are not discriminated against or disadvantaged and that you do not necessarily lose your leverage off each other. That is where I talk about the link between regulation and law enforcement.

A classic case might be where you have got a central authority which issues licences in respect of certain kinds of financial institutions. The licences have certain conditions attached to them, as to what a financial institution might do. If there is very effective communication and coordination between regulator and law enforcement agency, the law enforcement agency can feed intelligence into the regulator, to let them know the sorts of activities that some financial institutions of this type might do which foster and facilitate illegal activity—for example, money laundering.

You might have a regulator saying, 'One of the conditions for licence for this financial institution is therefore to do certain things,' so that their business operations are hostile to being used for those illegal purposes. So you have a really good interaction between the two. That is a very simple example and that is one that already happens in the Australian context anyway. But if you widen that out much further to issues such as when telecommunications companies are entering our markets—and it is going to be a deregulated market towards the latter half of this year—then, in setting up those markets and in fostering that, government thinks about the way in which telecommunications services will be used in relation to, say, the financial sector.

Another example is the Internet service providers. They are coming through, they are providing a service. They were traditionally providing just a communications method for Internet buffs from one corner of the world to talk to those in the other but, very clearly, they are going to take on much bigger roles over time, including providing the conduits for financial services.

So all those sorts of issues that come up in terms of what is the role of ISPs in relation to pornography on the Internet also come up in a different context, but with the same principles, in relation to things like money laundering over the Internet. So no-one is an island—that is what we are trying to say in this report. The issues that are of concern to law enforcement are of concern to many other parts of government from their own particular perspectives.

CHAIR—Just on that point before you answer the question on the powers, you are advocating a whole of government approach. I assume you are saying that at the moment we have not got a whole of government approach. That is not a criticism of the government but it is a fact because we are catching up. I take it that the Electronic Commerce Task Force is a one-off. That was a task that was given to your organisation; that is now complete. But what in practice is needed now from the perspective of a whole of government approach? A department within a ministry? What exactly are you saying?

Ms Montano—This was a one-off. It was a 'let's explore the issues' document and

that is why it does not come to many conclusions. I think our recommendation No. 1 basically gives a very broad outline of a suggestion that there be a central point which coordinates the involvement of many different aspects of government policy makers. I am obviously not talking about what the policy would be; I am talking about the process by which policy is developed and that definitely will need the input of a whole range of areas of government.

If you look at the list of contributors to our report, we attempted to go out fairly widely within government to get as many people as possible to give their perspective in a working party situation. That was moderately successful. We had some time constraints against us in terms of people being able to really provide valuable input from some quarters. We tried to emphasise, particularly in the preamble, the fact that this is a new phase, as it were, in government and the way government reacts to the societies it governs.

Back in the early days when you had a little village somewhere, you had whole of government simply because everyone who stood there was everyone. So you got whole of government consideration of issues merely by the fact that we were all there. Obviously, as societies get more sophisticated, government fragments into particular tasks and responsibilities and, understandably and quite logically, specialisations develop in relation to consideration of issues.

What electronic commerce has done, and particularly things like the Internet and the ability that has to be used for a whole lot of different functions, is that we are almost going full circle back to a need to sit down all together and say, 'We have got this thing here. It is not only important to one person in the village, it is important to everyone. What's more, it is not only our village; it is the village across the hills and the one over the sea.' We tried to take a fairly historical and almost jurisprudential look at the way in which we thought law making and policy making was going to have to develop. So that is the basis for that recommendation.

CHAIR—Could you comment very briefly on the powers of the authority?

Ms Montano—We had a very quick look at the powers of the authority in the context of law enforcement generally. Certainly things like the coercive powers and so forth stand and they are obviously very effective powers. The things that we were very concerned about were the very traditional and standard techniques and methodologies that law enforcement uses and how they would be superseded and become ineffective. It is not only an NCA issue; it is a wider issue.

But we thought that with the NCA in particular there were some fairly important issues in relation to money laundering and organised crime, because the kinds of organisations that the NCA is targeting are obviously those that are sophisticated and which will have access to a lot of this material we are talking about. They will also be earlier to pick up on it than many other criminal groups which other law enforcement

agencies might have a focus on.

So we are very concerned about things like the interception powers. What I think will inevitably happen—not very soon but it will happen—is that the telephone intercept, which is very fruitful at the moment, will become less fruitful when criminals are conspiring and planning over the Internet with encryption systems in place. Not so many years down the track everyone will have a PC in their house. Everyone can link into the Internet because that telecommunications carrier we were talking about earlier is now providing very cheap and accessible Internet connections. You do not have to go to a special ISP to get Internet services. Your telephone company will say, 'Look what we can offer you—a range of services, including Internet connections—and it is very cheap.' So they will conduct their conspiracies, as it were, by Internet. One of the classic ways in which law enforcement generally and the NCA in particular has had success is telephone intercepts.

We are also concerned about even more traditional things like informants, witnesses, people who see the 'deal' happening, in the sense of the money changing hands, if not the goods. You might still have to have physical delivery of the goods but the payment might well be via means of a card swiped down the slot of a phone and a few minutes later it is then offshore as well.

So all the assumptions that our law enforcement techniques have depended upon, which were very logical and reasonable assumptions and they are very successful, are being challenged. It is a question of how we can get back to the basics of what the objective is and, with the new technology in front of us, where the vulnerable points are going to be where law enforcement can appropriately tack in.

Mr SERCOMBE—I was wondering if any of the three witnesses could perhaps give us some views on where Australia is in an international context in relation to dealing with the gamut of issues that we are talking about. Quite obviously, any developments in this area not only have to be whole of government but they also need to be multi-jurisdictional to be effective.

As I understand it, Australia is fairly widely regarded as very much at the forefront internationally in respect of financial transaction reporting in legislation presently. But even within that context, the fact that the Cayman Islands are there, the Isle of Man is there and Liechtenstein and a range of other jurisdictions are there, mean that even within the current technology, in the absence of further progress on an international level, there are significant limitations. One assumes that they are going to broaden out and get significantly greater as new technology unfolds.

So it would be helpful to get a sense of where Australia's position is and what is occurring internationally in respect of this. I understand that the G7, for example, has a financial task force operating as well. Just some briefing on where we are at would be

helpful.

Ms Montano—Perhaps I will say something and then leave it to people who have more expertise in the particular technologies. You are right, Australia is perceived to be a world leader in some kinds of this activity. For example, the transaction reporting regime is very sophisticated. The G7 group is the Financial Action Task Force, of which Australia is a founding member. We were reviewed by the FATF last year in an evaluation and were found to have the most sophisticated systems. That is largely due to our existing use of information technology, the way in which we capture the information, analyse it and send it out. That is one of Austrac's functions.

The position is that Australia is very well regarded internationally in this whole area. My assessment of other members of the FATF is that our research into this is at the head of the pack in respect of looking at what this means for government and particularly for issues like revenue. We have been liaising pretty closely with counterparts in the US. They are at very similar stages of thinking about the issues. They are still working out exactly what the government role is in this and what to do about it.

So, technically, we are very much at the front at the moment. But there will be dangers if we do not continue that work, because we will end up with the systems we have being bypassed. They are very much based on the way in which the financial sector works today. The financial sector faces a big revolution in the next five years or so—growth of Internet banking, all those sorts of things, and the rise of other intermediaries. We will find that the ways in which we assess things will be gone, so we will have to move.

Mr SERCOMBE—I appreciate that background and understand it, but how effective is all of that in the context of Australia and a number of other countries, perhaps including the US, which have an effective regime in place? Does it simply mean that transactions go to other jurisdictions? So a huge investment can occur and catch a few mugs, but anyone who is reasonably sophisticated is simply going to avoid the jurisdiction, aren't they?

Ms Montano—If one of your aims is to make people want to avoid your jurisdiction so as not to use you as a money laundering conduit, then you have achieved your objective by having a system in place. Certainly, one of the messages that we put out is that Australia has a system which is there to deter anonymous large-scale transactions. If the Cali cartel is making a business decision on where to open up a new market and a very big part of that business case is, 'How do I get the money out and how quickly can I repatriate it to Colombia?' then certainly that is one of the important issues.

Mr SERCOMBE—Good point.

Mr Wahlert—As to the question of where we are in the world and the

consideration of these issues, we have been in constant contact with a number of law enforcement agencies around the world, particularly in the United States and Europe. We have been surprised to find that in fact we are at the forefront of consideration of the issues.

As to where to go from here, we have to tread very warily because many of these systems are embryonic. They are only just emerging. Their exact form and shape have not yet been identified. So we have to look very carefully at how they are likely to emerge in the future. Even to the point of public acceptance and the marketability of many of these products, there is still a question mark next to them. So how big they will become, and, therefore, how much of an interest they will be to law enforcement, is still being looked at.

One point I would make, however, on the Australian environment and our consideration of the issues is that we are working very closely with industry, which is a very positive sign, in the identification of some of the law enforcement concerns. They have been very receptive to what our concerns are and how they can perhaps work together with us towards coming up with practical solutions, such as reasonable limits on the amount of certain transactions and the amount of money that can be transacted, et cetera, with these new systems.

Dr Grabosky—I want to briefly mention the issue of what you might describe as computer hacking, or electronic vandalism as we refer to it. Australia seems at this stage not to be as attractive a target for that kind of activity; nowhere nearly as attractive as the United States, for example. In the past year, the Web pages of the US Department of Justice, the Central Intelligence Agency and the US Air Force have all been defaced by intruders. There is no end of people who devote a great amount of time and effort to trying to penetrate the systems of defence installations in the United States. Australia appears to have been spared that degree of attention thus far.

I think one lesson from all of this is the importance of computer security, which it seems to me will be one of the growth industries—if not the growth industry—of the early 21st century. There are technologies and systems that one can develop to minimise the risk of some of the misfortunes that have been experienced abroad. That, to me, seems to be one of the key lines of defence against electronic illegality of many kinds in the years to come.

CHAIR—Thank you.

Mr FILING—If I can just look at recommendation No. 8 in relation to the treatment of the Internet. Post-July this year, with full deregulation of the telecommunications system, it is going to be far easier for Australian telecommunications users to access call-back lines and cheap calls outside of Australia. The trend is going to be towards more and more data compression using the new higher speed modems that

require compression, because they are going over twisted copper pairs. How on earth do you expect to be able to enforce any regulatory framework given that people who want to avoid Australian jurisdiction could do so perfectly easily?

In fact, I would have thought it is almost impossible to enforce a regulatory framework. The domain names can be obtained outside of Australia; there is no need to use Australian regulated domain names. You could set up a domain anywhere in the world that is available to you at the right cost and, presumably, the requirement for entities trading on the Internet to be required to identify themselves to standards consistent with established practices and requirements is almost laughable.

The workload to be able to police that would be almost impossible to cope with. I share your objectives, but I am just wondering about it. I might just say, if I may, on the last point about ISPs being required to operate from nominated premises, if an ISP is operating offshore, how on earth do you intend to enforce that?

Ms Montano—Many of our recommendations work on the basis that this is seen to be part of a fairly global approach. We know that we are not going to get every country in the world to agree to impose these sorts of requirements on the Internet users and providers, but the theory is to try to encourage, as much as possible, a fairly ordered way in which these things occur.

What we are really doing is taking the basic principles that apply in relation to, for example, companies—know who are the directors behind companies, have the ability to enforce contractual rights and so forth against people because you can go to a register and find out where they are supposedly. That is not a foolproof system in our current world anyway, but it is seen to be a way in which you can translate some of those business certainty principles into this new environment.

You are quite right; anyone can set up an Internet address anywhere and broadcast worldwide and transact with people worldwide. That is where we see some fairly important roles for the industry itself and also very educated market participants in that, when you see a domain name and an Internet address which comes perhaps from a particular country or perhaps from a particular region and you know that that country does not subscribe to some international code in relation to the regulation, then it is very much 'buyer beware'—please be aware that the entity you are dealing with may not subscribe to a particular code or be subject to certain regulations in respect of your being able to find out who you are really dealing with.

Mr FILING—I apologise for missing the beginning of the hearing. Can I go back to the actual definition of financial transaction. A person who is selling, let us say, shareware in California can ask you to send card details to complete a financial transaction to purchase their software. That is a financial transaction; it is capable of being used for money laundering relatively easily. I would have thought that that is likely to comprise

about 90 per cent of present transactions occurring which are those sorts of straight purchases of services of one sort or another. All of those are able to be used as money laundering instruments in a money laundering technique.

I would have thought you would probably be far better off devoting much more resources to ensuring that Australian users are more acutely aware of the likely pitfalls of transactions of those sorts. If somebody puts their card number onto the Internet they know, at present, without the benefit of the new security arrangements, that they can have their card details hacked and used by somebody else or that people can try to use those card details for other transactions. But on their Explorer software engines people are generally warned about putting their details onto the Internet, but that is going to change very shortly with better security arrangements with the new software that is becoming available.

I think that it might be almost a mission impossible to try to enforce a regulatory framework. You have mentioned letting the buyer beware and market forces are perhaps becoming a greater influence on people's behaviour on the Internet. Would it not be better, instead of trying to enforce a perhaps unenforceable regulatory framework, if more resources were devoted to perhaps informing and educating people about the sorts of things that can happen when they enter into transactions on the Internet with entities with which they are not familiar?

Ms Montano—Certainly, you are quite right. That is one of the strategies I mentioned early on—that there would be far more scope for self-regulation and co-regulation and the market saying, 'Here is an issue. As market participants, we may well want to impose a particular code of conduct and also have things like educational programs.' Certainly, the best tool a regulator and a law enforcement agency can have is an aware, astute and sophisticated would-be victim so that people know that, when they go into the Internet, there may be someone who will say to me, 'If you would like a free download of pornography, just press this button.' There is a lot of publicity coming out at the moment about where you do that. What you get are viruses that come in, search through your database, work out if you have certain programs in relation to payment facilities, and they will then make payments offshore to accounts in the Cayman Islands or wherever. What you have to do is get a fairly educated market and, unfortunately, probably a few people who have been burnt and who are brave enough to say they have been burnt, and you have a very effective deterrent to people doing that sort of thing.

The industry itself is very aware of the dangers and that is why there is such a big push to establish free information services in relation to the abuse of the system. So we see that as being a very important part of that, and the regulator's role is to say, 'We are encouraging people to be educated and sophisticated users of these technologies. Reap the benefits but don't be foolish enough to be caught in terms of the downside of being a

victim.'

Mrs WEST—I would like to know if there is a national register of Internet users. Does anyone who wants to use the Internet log on to a central register of users? Is there anything like that at all? That is the only way I can see for you to regulate or review who is using it.

Ms Montano—You go to an Internet service provider, who may be one of the big established groups or may be a small outfit. You pay your fee. You get allocated a name and you trade. You do business.

Mrs WEST—There is no central register of who is on it?

Ms Montano—No. It is very hard for them. They are a very aware and responsible group in the main—in the sense that they are concerned about what goes along their lines. They are not able to be the censors, as it were, in relation to the material that goes down the line. All the submissions and so forth they make in respect of things like inquiries into pornography on the Internet apply in exactly the same way. It is a different subject matter but the same principles apply in relation to things like, 'Well, we don't want you ISPs to facilitate money laundering,' and they are going to say, 'Well, how on earth do I know whether a transaction is money laundering?'

The beauty of the Australian system is that we have a very free and open financial system. That is a big advantage and it is something we have to do if we are going to be a significant world player. But with that comes the fact that people can disguise transactions to look legitimate. By the time you had explored a particular transaction to see whether in fact it was or was not, it might well have been and gone; you are wasting your time.

Mrs WEST—What would you consider to be the first step towards regulating use of the Internet for the government showing signs of having some control over what is going on on the Internet?

Ms Montano—There is a series of things that would have to be explored at the same time. Mr Filing is perfectly correct: you have to do it internationally; we cannot just do it domestically. It is a question of working with the providers to see what they can require of the users of the systems that is not so onerous that you end up with the compliance costs being unreasonable and interfering with the way in which people are going to do business.

It may well be a question of just requiring Internet providers at the beginning of the process to set up the systems whereby you at least have something to start with as to who is operating under a particular domain name, and it is then a matter for law enforcement, for example, to negotiate in relation to things like tagging of particular kinds of transactions, to do some kind of traffic analysis.

We do not know now for sure how to do it. We think we know the ways to explore to do it, but we do not know exactly what to do, simply because the systems themselves are still being developed. For all the huff and puff, the Internet has not yet achieved mass market penetration. It is going to. But at the moment, it has not.

I think that once the security issues that have been referred to have been sorted out you will see a big explosion in the use of the Internet for financial transactions. There are a lot of people who are very wary about things like putting their credit card details on the net. When I put that to a lot of computer experts, they say, 'Well, the chances of someone picking out my transaction with my credit card details in a flow of information is fairly slight, and I'll run the risk.' That is a question of an individual knowing the risks and choosing to assume them. But certainly there are a lot of people who are deterred from doing that in the meantime.

Mr Wahlert—Can I add two things. First of all, in relation to Internet service providers, the ones in Australia, particularly the larger ones, have a very good relationship with law enforcement, or we certainly do with them. In the main, they are not the problem. The main problems we are having, although there is no real baseline data, are mainly with overseas entities—be they overseas service providers, overseas groups et cetera. It is not so much the case in Australia.

Also, in relation to what we can do to make the Internet a safer place, I think many of the necessary environmental factors or controls are being introduced by commerce. We have got things like secure electronic transactions, or SET protocol, to enable safer transactions, or relatively safe transactions, over the Internet using credit card details et cetera.

So the infrastructure is being developed now. In the main, it is being developed by commerce, because they have a vested interest in ensuring that the Internet is safe for commerce so that they can make money.

Mrs WEST—From a government's point of view, would you see a central register of all users being feasible or viable?

Mr Wahlert—I do not know how feasible it would be at this stage. Maybe it would be in due course, but I do not think it is feasible at the moment.

Ms Montano—If you think about the systems we have now, we have company registers of directors and so forth, but it does not stop those people doing things. That is a case where we would say that that might well be over-regulation or, rather, regulation that does not really achieve anything at the end of the day. We do not know yet, to be honest.

CHAIR—Counterfeiting has been a problem and Australia is right at the forefront

of preventing that with our technology, but it seems to me that we might have wasted a lot of effort there. What is the potential for the use of the Internet for counterfeiting activities? I am trying to get my mind around this. Electronic banking to me is still a hole in the wall or EFTPOS. We seem to have gone leaps and bounds beyond that already.

In terms of the use of the Internet, could you explain in practice how we are going to bank on the Internet and how you prevent counterfeiting type activities or money laundering activities on the Internet? When you talk about money I see dollars and cents and so on. I am trying to imagine what the potential is for use of the Internet for counterfeiting and money laundering.

Mr Wahlert—In relation to counterfeiting, the key is the encryption technology that is being used to protect the information—the zeros and bits and pieces that make up the digital money. Organisations and companies are looking to introduce a digital analog of cash and hard currency as we have it today. They are aware of the potential problems in relation to ensuring the integrity of their algorithms—the cryptographic keys that are protecting their systems.

We do not yet know what the threat is going to be on those systems in due course. Companies such as banks are very effective and have very good risk management in working out what the risks are but this is a new world, and I do not pretend to have the answers to that. Certainly, I think we are going to see the developers of new encryption in a headlong race to keep a step ahead of the decryptors—the people out there who are not just criminals but perhaps hackers who are looking at it as a challenge to break someone's keys. As computing technology increases, so the capability to decrypt and encrypt will continue to race forward.

I think we can also see the possibility of these systems being attacked by all sorts of people. Again, industry is aware of this. It is aware of the potential problems and is doing some very good work on ensuring the protection of digital money.

Specifically on counterfeiting, one of our concerns is—again, we do not know how big a concern this is likely to be because we have to wait for the market to develop—that if you are able to crack the algorithms or the encryption protecting a digital currency and duplicate a digital coin then, unlike a real note which has a hologram, texture, a number and metallic strip et cetera, where you have a chance of detecting counterfeits, this is not necessarily going to be the case in a digital world inasmuch as a duplicate is every bit as good as the original. Also the ability to see counterfeit digital currency is another problem. Again, we have no idea of what the magnitude or likely potential of that concern will be.

Ms Montano—What we are looking at is also encouraging the entrepreneurs to provide systems. For example, let us say someone counterfeits a token with monetary

value. We can suggest—and it is in their interest to do it themselves in their preliminary work—for example, that they have systems running so that when that value is returned to the central system, when that value is given a unique identifier number for the purposes of tracing funds around the system, perhaps there are triggers in relation to the second time it comes back, in that the same thing cannot be in two places at once, so therefore we trigger an alarm.

That may well detect activity. It may not help much in working out who it was who has passed it and which one of the multiples that have been passed through the system is the legitimate one and which are the copies, but it is those sorts of techniques that we are encouraging them to build into their systems. Glenn is quite right. It is a question of making systems as difficult to infiltrate as possible in the first place.

Senator FERRIS—Could I ask a slightly futuristic question which I would like each of you to respond to, if you could? Firstly, in his paper, Dr Grabosky says on page 6:

There is a significant danger that premature regulatory interventions may not only fail to achieve their desired effect but may also have a negative impact on the development of technology.

Then, if we go to Mr Wahlert's paper, on page 4, talking about regulation, he says:

In many of these cases it is very difficult to resort to pre-emptive regulation as a resolution of issues we have not as yet identified.

The first recommendation of the nine in the ECTF report, with a rather daunting array of break-outs from the first one, suggests:

Recommendation 1: Establishment of a Task Force to oversee whole of government reform program . . .

Perhaps looking five years ahead, what would you see this task force being able to achieve, given the comments that have been made in your papers about the dangers of regulatory reform? Yet (i) says:

(i) examine and formulate policy on the basic issue of what the role of government is in this area.

If you accept the basic premise of government to set frameworks for the operation of industries, in five years time what would you see this task force achieving if you were in fact to set it up and proceed with these six tasks? Could each of you respond to that?

Dr Grabosky—Perhaps I could start. I have not had the benefit of reading this report. I can at least advance that excuse if my response is inadequate.

Senator FERRIS—Page 111.

Dr Grabosky—It seems to me that in five years time the technologies of electronic commerce will have developed significantly beyond the current state in terms of their penetration, their security and their acceptance in the community. At this point the shape and the trajectory of the technology will be a little bit more apparent. I think at that point one may have a handle on, for example, the degree to which electronic transactions are transparent, traceable and by whom and, at the same time, which aspects of transactions should be private and inaccessible. It is only as the technology begins to emerge that one can get a better handle on how and when to intervene, if intervention is possible and appropriate.

Senator FERRIS—What you are essentially saying, though, is that the government would have a catch-up policy.

Dr Grabosky—Yes.

Ms Montano—I do not think any of the three statements you read out are inconsistent. What we are saying is that it will have to be a fairly laid-back approach. The group that we were putting forward, as perhaps a suggestion as to how this might be done in practical terms, would comprise and be heavily reliant upon the market in terms of government objectives in broad terms. It is not difficult to set out very broad government objectives and the role of government. The role of government is to foster and encourage the development of systems which are credible, safe and provide equal access to all. There is a whole range of things that are nice social objectives which no one could challenge as being the appropriate role of government or appropriate objectives.

It is in the mechanics—when you come in, and when you do not, and how you achieve that—which is where we are going to have the difficulties. That is a question of saying, 'Okay, we all know what our objective is. Our objective in relation to all stored value cards systems is to have a credible, prudentially sound system which will encourage use, because we see that will lead to decrease in some kinds of crime. It will facilitate commerce and so forth.' The features that society is looking for in relation to a system like that are things like safety and soundness as to the investment people have made by handing over their money in exchange for value on the card and so forth. You would end up having a whole range of very broad indicators.

Then, for example, you would give that to a group which comprises government and market and say, 'There you are, you go and formulate a series of general guidelines'—which will probably be very general so as not to favour one technology over another—'which say, "Okay, in your systems, we would like to see these kinds of features."' How you technically achieve that is a matter for the market, but government has a baseline for what it wants these systems to have. So it is regulation, but it is far less prescriptive than we have traditionally seen.

It is a bit like drawing an analogy between the Corporations Law and the old

Companies Act. The prospectus provisions under the Companies Act used to have enormous lists of things that had to be in a prospectus, things that were determined by government to be important for the investing public to know prior to making an investment decision. They were amazingly prescriptive but were very good. They were developed over time, with the benefit of a lot of experience and a lot of understanding of things that had gone wrong in the markets.

But that in itself had an effect on the market in the way in which prospectuses were developed. Check list mentalities operated. The corporate affairs commissions were seen to be the last port of call in terms of the last quality check for prospectuses before they were issued. So it was almost as if the onus was on government to raise capital.

What the Corporations Law did was turn around and say, 'Hey, you—the directors and senior advisers—have the expertise and the knowledge'—in relation to a particular offering—'to know what it is an informed investor needs to know. Therefore, with a very small group of basic requirements that are prescribed, you have to say what it is the informed investor needs to know.' The market then had to say, 'Okay, I am a person who wants to invest in a certain product. What is it that I would want to know?' So they had to develop their own prospectuses. It is similar in the sense that you then leave it to the market. The government has set an objective: an informed market. How to achieve that is up to the market participants and those who wish to go out and raise capital in the market.

There were teething troubles along the way. I used to be with the Australian Securities Commission, so I have a perspective on this. For the people who still wanted to be told by government how to do it, government issued guidelines and so forth via the Commission. But, basically, the market now has a view as to what it is it has to do to achieve that government objective.

It might well be that that is the way this will work. There will be periods of uncertainty along the way, but government will have to be very clear about general policy directions. The market will have to work it out. The markets will do it very quickly because they need to survive. A government directive is, 'Systems that wish to operate will need to have these following basic features.' The first thing an informed investor will say to the promoter is, 'Can you tell me how you address those basic requirements?' They will have to prove to the market the worthiness of their product.

It might be that that is the way it is. So we have government not being prescriptive as to how to do it and not trying to favour one technology over another, but it is saying, 'You, market, go and do it. Here are some guidelines and here's a general framework.'

Senator FERRIS—So you are suggesting that it would be proactive, whereas Dr Grabosky was suggesting that it would not be perhaps reactive but that certain difficulties or problems with compliance would be identified by the market and the government would come in behind to look at whether some more complex form of regulation would be

required.

Ms Montano—It is always a function of government not to be too prescriptive but to come in afterwards and see what a market has done and try to do something. That is inevitable.

Senator FERRIS—But we are dealing here with an industry which each of you earlier identified as being a picnic for criminals. It just concerns me that we may need to have a huge market difficulty, which might be identified by the NCA or some other crime enforcement body, as a result of which somebody would suffer before we are able to identify the framework that is going to be needed. Mr Wahlert, do you have anything to add?

Mr Wahlert—Yes. As to prescriptive regulation, I guess I am advocating in this paper a 'hands-off, eyes-open' approach. In some ways that is pragmatic from a law enforcement perspective. We are not too sure yet how law enforcement processes are likely to work in this emerging environment. Considering that what law enforcement in part does is attempt to control behaviour, that is very difficult to do on something like the Internet. So one of our concerns is that it is one thing to have regulation; it is quite another to be able to enforce it.

I will go back to the original question. If we put ourselves out five years—in the year 2002, an arbitrary period in the future—and look back at what this task force could have achieved, I think we would find that there are some practical things that we can start planning for now to be ready for this emerging environment. Some of those have been identified in the paper, such as working more closely with industry, sharing our ideas and concerns and making them aware of what some of the potential pitfalls are, if they are not already aware of them—I am sure they are. Specifically, we could look at how regulation may assist them and perhaps come up with a bipartisan approach within law enforcement industry groups to what an effective regulatory framework might be.

As importantly, we need to work with international groups because this is a borderless international environment. We need to ensure that whatever regulations we have, or even self-regulation controls, are entirely appropriate internationally, that they fit in with other organisations around the world. As Ms Montano said, we are not an island; whatever we do must be practical on an international basis.

CHAIR—We are scheduled to finish at 10 o'clock—I said 10.30 earlier by mistake. I am sure you have other commitments, as we also do. If you do not mind, we will just go on for a few more minutes.

Mr SERCOMBE—Mr Chair, noting what we all acknowledge has been the essential uncertainties of a great deal of what we are talking about, and also noting the importance of self-regulation, as Ms Montano has talked about, I nonetheless would find it

helpful to have our witnesses talk a little bit about the resource implications for the Commonwealth of some of the things we are discussing.

For example, I notice that in the report there is a section on inter-agency, international cooperation. The report makes the fairly alarming comment that it is certainly likely that law enforcement will become increasingly reliant on a range of national security capabilities and skills, such as cryptanalysis, electronic surveillance and interception.

Taking into account what Dr Grabosky said before about the balancing up in a democratic community of things such as privacy and the like, that sort of comment also has massive resource implications for the Commonwealth. I just wonder—particularly as to the experience at the moment, where fiscal rectitude, in the government's mind, is making the task of law enforcement very difficult in a technological sense, apart from anything else—how you see the resource implications of the sorts of things you are talking about imposing on the Commonwealth?

Mr Wahlert—Yes, there are bound to be resource implications, but it is very difficult at this stage to quantify exactly what those implications will be—again, because we have a very hazy picture of how this environment is going to emerge. As to working more closely with national security organisations, and perhaps even defence, yes, we can see that perhaps occurring. It is occurring already to a degree. In some ways that is maximising the use of resources to the benefit of the nation rather than giving law enforcement additional resources and additional powers. I think that is likely to continue for some time, until it becomes clearer exactly how these environments are going to shape, what form they are going to take and what specific things law enforcement can do to address some of the problems that are on the horizon.

Mr SERCOMBE—Are we talking here about massively expensive technologies for the Commonwealth?

Mr Wahlert—Some of the technologies that provide a technological solution are exceptionally expensive. But I do not know that, at this stage, it would be prudent to look at utilising those technologies.

Ms Montano—The other thing is that a lot of those technologies are developed in a national security context anyway. It might well be that, yet again, it is a question of a bit more cooperation and interaction between various spheres of government whilst obviously keeping in mind the very clear roles and the safeguards you have to put in place as to the way in which government exercises power.

As for resources, yes, I think it probably does mean a very serious look at resources, but if you look at the overall issue we are not talking about law enforcement alone.

The other aspect of all this—and a very important thread and one of our recommendations—is in relation to looking at revenue consequences for Australia in this area. There are significant and persuasive arguments for a very serious look at this from a revenue perspective. At the moment, if you look at the international tax treaties and the arrangements that are in place, again the assumptions they rely upon to determine and to cut up the cake, which could be international tax revenue, all depend on things like residency, source and a whole lot of rules which historically make a great deal of sense but which, when you start to look at the way in which people can conduct business, particularly over the Internet, we will have to rethink, and there will have to be some agreements and a lot of horse trading done at an international level in relation to cutting up that pie. The more we know about it and the more research we do, the better equipped we will be when we go to those negotiating tables to work out what it is we are agreeing to or not agreeing to.

Mr FILING—Even a domestic transaction may actually involve packets of data travelling over several countries. In whose jurisdiction would an offence take place?

Ms Montano—That is a matter for negotiation between the countries concerned. There are lots of issues—

Mr FILING—Let us say one of them is over the phone lines of, say, Turkey, which is a bit of a rogue state in terms of international policing agreements. Where would the jurisdictional application of laws apply?

Ms Montano—At the moment or what they might be?

Mr FILING—I am looking at the present, where we are looking at a prospective regulatory framework over something that, in my view, cannot be regulated.

Ms Montano—You are right in the sense that, unless and until you get every sovereign state in the world to agree to a particular code, you are not going to get blanket coverage. But there are ways and means by which countries who do subscribe to a particular way of conducting this business can put market pressure on certain countries or on the way in which markets behave.

For example, let us talk about the way people deal with tax havens now. There are some businesses and individuals in Australia who channel funds out to tax havens. Response to date has been to say, 'All right, if you are going to send your money to a tax haven, there are certain rules and certain ways in which we will treat that money.' For example, you have withholding tax and you have things where you make an assumption that, unless you are going to subscribe to and be governed by the jurisdiction of domestic tax laws, then certain rules will apply in relation to those funds whilst they are in our jurisdiction. So you might have variations on that sort of theme.

You might have situations where, although we are moving more and more towards free trade and so forth and that is a very desirable outcome, it may well be that some countries take a view that there are countries to whom they will not give favourable treatment in relation to certain parts of their economic systems because of the way in which they will allow their countries to be used as bases for certain kinds of transactions.

I can give you a fairly dramatic example of the way in which this can operate. It came to the attention of the Financial Action Task Force that the Seychelles was going to introduce some legislation which could be seen as fostering money laundering activities in that country's banking system. Certain members of the FATF took the view that they did not wish to encourage that—they could see some of their own domestic arrangements being affected by that sort of facility being available to its citizens—and therefore took a view that, 'If that is the way you want to conduct business and to set up your legislation, then it may well be that the clearing houses and the financial infrastructure of another country will not be available to your banking system.' That is a dramatic example but it is one which meant that the Seychelles legislation is not being proclaimed and is said to be on the shelf.

Mr FILING—There was one argument earlier which I wanted to press you on—I think it may have been Dr Grabosky's argument that if you introduce a regulatory framework you may in fact retard the development of information technology in a country. I put it to you that in all examples where a government imposed regulatory framework impinges on technological development it has in fact retarded development in the country of jurisdiction.

An example is Brazil, the one I have seen first-hand, where they had a regulatory framework on computer developed hardware and software which effectively set Brazil back about 10 years behind most other countries. Would you agree that the danger is that any, let us say, heavy-handed regulatory framework is likely to retard Australia's development as a state-of-the-art information technology country?

Ms Montano—I think we have all said it at various times. I think it is something that is a given. If you over-regulate and if you distort the markets and the development of the technologies, then you are defeating your own purpose—and that is to have systems which are in fact buoyant and resilient and strong and innovative. It is a given, I think, and that is why our advice is to very cautiously move forward.

Mr Wahlert—And not those in regulatory environments and not developed in isolation from, say, industry. We must have wide consultation with those groups.

Mr FILING—If there were an international agreement on a basic set of rules for ISPs, for domain users, for basic credentials for business entities on the Internet, they are more likely to be far inferior to Australia's current corporate regulatory framework. And that is likely to have an effect of reducing Australia's corporate regulatory framework

now, or it would distort Australia's corporate market by reducing the standards, because naturally there are going to be countries within the framework that we are looking at whose standards are completely lower than Australia's in relation to corporate regulation.

So any compromised, international regulatory framework is likely to lower the standards vis-a-vis Australia, which will in effect lower Australia's own standards, because companies that have Australia's present corporate regulatory framework imposed upon them are likely to see what is available on the Internet and elsewhere and look to those because they will be less onerous and less expensive.

Ms Montano—It is called regulatory arbitrage, where you jurisdiction shop for particular things—and that is a phenomenon which regulators are well aware of, and that is why it is even more reason to ensure that as far as possible you negotiate reasonably tough international standards. If there are players who do not wish to abide by the standards, which there will be, then the markets themselves will, as I said, give signals in relation to what it means to trade with entities coming out of places which do not have as high standards. It will be a market beware, buyer beware, situation.

Mr FILING—What I was trying to say was: do you not agree that in essence an international agreement is going to in effect lower Australia's standards?

Ms Montano—It depends what the agreement is.

Mr FILING—I know. Are you sure that we can regulate it for sure? In fact, it is probably a bit of a pipedream to look at a regulatory framework on the Internet of any substantial effect. But given that there is a regulatory framework in the future and that in that framework entities are able to trade legitimately as part of the international agreements, then I would put it to you that in essence that is likely to be far inferior to Australia's current regulatory framework and the undertakings required of trading entities presently in Australia would be far less on an internationally regulated Internet or electronic trading market?

Ms Montano—If it was only government that was setting the standards, then that might be right because we have a tradition of fairly high standards in relation to transparency and honesty and openness of markets. But the reality is that the markets themselves will be looking to raise the standards because, if you look at the material that the market participants themselves are producing, they are very conscious of the need to prove their products as being ones that are worthy of confidence, to get the mass penetration they need to make them commercially viable.

So it will not just be government that is saying, 'We need to know who is doing what so that we can have orderly markets and we can have orderly contractual arrangements,' it is the markets themselves—for example, the private legal profession. When you start to advise people in relation to transactions on the Internet, the series of

five or six basic questions that I, as a private adviser, would be asking my client to be satisfied about before transacting on the Net are very similar to the ones that government will be asking: do you know who you are dealing with; if you know who you are dealing with, where are you going to deal with any disputes—what jurisdictions, set of laws and rules in relation to basic principles, evidence and so forth—and whose laws are going to rule any dispute you have; whose laws are going to work out whether, even if you get a judgment, you can go out and take actions against particular assets; what are your remedies going to be in a practical sense? All those sorts of issues that the private sector will be asking to be satisfied about before they go and actually transact seriously on the Net are exactly the sorts of things government will be concerned about.

Mr FILING—The reason I ask is because, if you looked at Australia's own micro-experience, let us say, with the corporate framework, in fact the transition from state based corporate affairs regulation to a national system has watered down the standards—in terms, for instance, of the opportunity for people who were formerly able to go to their state based corporate affairs jurisdiction and get some redress in the case of where they have been defrauded or where people have violated the companies code in their particular state. Now it is almost extraordinarily difficult for them to get it unless they reach a particular threshold of the value of the transaction. What I am saying is that when I was—

Ms Montano—I do not think that is only a national issue. I think that has a lot more to do with resources and other priorities that are assigned to people.

Mr FILING—The purpose of the hearing was to look at this from the point of view of Australian criminal law enforcement. What I was saying was that if you looked at an international framework for corporate regulation for trading on the Internet or on whatever electronic market it was taking place, then in essence you would water down the corporate regulatory frameworks, rules or the requirements to a compromise lower standard to accommodate countries which have far lower standards than Australia, who would be, naturally, trading. I am looking at countries such as Switzerland; countries where there are lower standards in relation to, for instance, declarations, information required of directors, et cetera, of particular entities. I am just signalling that perhaps—

Ms Montano—That is a danger. It is a danger that you would get to lowest common denominator in the course of your negotiations. I think that is always a pitfall.

Mr FILING—If that happens, then that will, by virtue of competition, lower Australia's own domestic corporate standards.

Ms Montano—If that is the only driver in the competition, perhaps yes. But I think that a lot of other drivers in the competition will be the desire of the markets themselves to seek out the places with the least risk. It will be like giving countries credit ratings. You give countries credit ratings and institutions credit ratings based on certain things. It does not mean that those with lower credit ratings do not play the game. People

will play with them but they will still know the greater risks they run.

Mr FILING—It will not be the countries trading credentials; it will be the traders'. Countries' interests will, I would have thought, be completely diluted. It is going to be who you are dealing with.

Ms Montano—The traders of a country which has low regulatory standards may well say to their own government, 'We are being discriminated against in terms of access to international markets because you, government, have a bad profile in relation to the way in which you regulate our corporate cowboys.' So, in that sense, you have a market drive to improve standards as well.

Mrs WEST—Where do we go from here? What is the next step? Is it recommendation 1, as my colleague suggests?

Ms Montano—The first recommendation of this task force was recommendation 1, and I think that is still a fairly appropriate way to go and, as to how that is achieved and whatever, then that is a matter for government.

Mr SERCOMBE—Can I take Ms Montano to the chapter in the report on evidence and proof. I thought that the general tenor of that section was presenting a fairly optimistic view about the likelihood of the Evidence Act, for example, in something like its present form and the general procedural issues in relation to prosecutions. It seemed to me that in the environment that you are envisaging emerging it was presenting a reasonably optimistic view about the situation at the present time and perhaps a somewhat minimalist approach to the need for change. Yet I would have thought that the recent behaviour of some courts in Australia in terms of success in getting convictions on complex matters, even in the current environment, would tend to perhaps belie what I see as optimism. Even the report under the discussion on smart agents, for example, talks about:

> In practice, of course, the prosecutor or plaintiff may face a difficult task in satisfying a court that the material produced by the smart agent was sufficiently reliable to be admitted into evidence. It is also possible that law enforcement authorities may be reluctant to disclose the extent to which they possess smart agent technology.

That is obviously a matter of some sensitivity to Austrac, but I think some people, including the NCA, are anticipating some circumstances where that consideration could produce some real difficulties. I wonder whether in fact you are optimistic about the current prosecutorial environment, I suppose, and whether in fact there is not a need for a more thoroughgoing examination, particularly of the Evidence Act, in relation to the new environment.

Ms Montano—I think what we were trying to do in that chapter was look at what the laws do at the moment and try to work out what we think will need to happen in the

future. The problem we have is that we have not had any cases run which have been thrown out, or which have failed, and so it is really hard to make particular recommendations for amendments.

We drew the analogy with the way the evidence acts have been updated over time to deal with, for example, that most business records now are held on computers. You have provisions in the legislation which say that the court will deem as good evidence the disk sitting there and, yes, judges and juries will accept the fact that that disk represents the following evidence when you reduce it to paper.

We were trying to show the evolution, as it were, of the evidence acts over time as the need has arisen. I think in a way it is a question of our having to work out the way in which the investigators find out what is going on, and then the next step in the chain is to work out how we get that made admissible in law. And that will mean that we will have to amend the evidence acts and the way in which the courts approach the issues. The problem is that we could not be more prescriptive than that at this time.

We were trying not to be too pessimistic in the sense that there will be ways—it will be a question of whether there is the will to make the amendments. You might even get to a situation where you have reverse onuses of proof. Historically, governments in our western tradition are very reluctant to reverse onuses of proof, except in quite extraordinary situations where you have seen things fail over time. And you get to a point where a government may well decide that in respect of some kinds of transactions they will reverse the onus or proof; they will put some prima facie rules into operation.

It is a question of using those existing techniques and just adapting until we find out is actually happening. The main author of this chapter, by the way, was a senior prosecutor from the DPP, whose brief was: 'Go out and think a bit more about how you would run a case like this.' And he came back and our discussions that followed showed that the principles are probably all there in terms of trying to work out how to do it; it is just that we do not know exactly what it is that should be done and it would be one of those pre-emptive steps to put anything in now.

So that is why a lot of our recommendations just say that we have to watch out for existing capabilities, that they are not watered down, and as we see the need we plug the gap. But that is as far as we could take it in terms of that, simply because we do not know how the courts will react to these sorts of cases and we do not know yet how they are going to be investigated fully and brought into the courts to start with. If the evidence that technically shows someone 'did it' is this particular thing or that particular thing, that would then impact upon how you get that admitted into evidence in court and then how it is challenged by defence and so forth. It really is a process over time.

Mr SERCOMBE—What about the process of discovery in terms of the technology that you might apply to accumulate evidence?

Ms Montano—The concept of discovery is really a litigious one between parties. Are you talking about Austrac activities?

Mr SERCOMBE—Yes.

Ms Montano—We do not discover in that sense. We have a range of financial transaction reports which come in. We analyse that at the moment because the reports are in English; they are not encrypted. They come to us electronically to reduce the costs and the time delays but the database is in English. If you know what the body is you can then apply your analysis rules and you can work it out.

The analysis rules that we will be applying in, say, five or 10 years time may not be much different from today. We have certain indicators of what is activity which we like to refer on to the NCA and other agencies for further examination. Many of those prove to be very good tips. It will not be that analysis function which will need focus but it is the collection function and the initial interpretation of what it all means that will need a lot of focus.

CHAIR—There is one technical matter for the committee. There have been three papers distributed by Dr Grabosky. Is it the wish of the committee that the documents be incorporated in the transcript of evidence? There being no objection, it is so ordered.

The documents read as follows—

CHAIR—Thank you very much for coming this morning. It has not only been fascinating and interesting but it has also been very important for us to understand some of these issues in a bit more depth. There are many challenges facing members of parliament but our particular focus is on ensuring the effectiveness and efficiency of the NCA. I think you have given us some excellent information and advice that we can bring to bear on our task in respect of the NCA. We very much appreciate you giving us your time.

Committee adjourned at 10.27 a.m.