COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE ON THE NATIONAL CRIME AUTHORITY

Reference: Law enforcement implications of new technology

MONDAY, 4 DECEMBER 2000

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

INTERNET

The Proof and Official Hansard transcripts of Senate committee hearings, some House of Representatives committee hearings and some joint committee hearings are available on the Internet. Some House of Representatives committees and some joint committees make available only Official Hansard transcripts.

The Internet address is: **http://www.aph.gov.au/hansard**

To search the parliamentary database, go to: **http://search.aph.gov.au**

JOINT COMMITTEE ON THE NATIONAL CRIME AUTHORITY

Monday, 4 December 2000

Members: Mr Nugent *(Chair)*, Senator George Campbell *(Deputy Chair)*, Senators Denman, Ferris, Greig and McGauran and Mr Edwards, Mr Hardgrave, Mr Kerr and Mr Schultz

Senators and members in attendance: Senators Denman and Ferris and Mr Edwards, Mr Nugent and Mr Schultz

Terms of reference for the inquiry:

The Committee will inquire into the law enforcement implications of new technology, with particular reference to:

a. whether use of new technology by law enforcement agencies is adequately catered for by Commonwealth, State and Territory legislation;

b. the extent to which electronic commerce facilitates the laundering of the proceeds of crime; and

c. whether international law enforcement cooperation is adequate to meet the challenges of new technology.

WITNESSES

Committee met at 10.02 a.m.

ALDERSON, Mr Karl John, Acting Assistant Secretary, Criminal Law Branch, Attorney General's Department

ELLIMS, Ms Sandra, Assistant Secretary, Law Enforcement Branch, Criminal Justice Division, Attorney-General's Department

HODGES, Mr Chris, Principal Legal Officer, International Branch, Criminal Justice Division, Attorney-General's Department

TREYDE, Mr Peter Richard, Principal Legal Officer, Information Security Law Division, Attorney-General's Department

GRANT, Mrs Marion, National Manager, Border Operations Branch, Australian Customs Service

NAYLOR, Mr Peter Charles, National Manager Investigations, Australian Customs Service

GRAY, Mr Geoffrey, Senior Assistant Director, Office of the Director of Public Prosecutions

MONTANO, Ms Elizabeth, Director, Australian Transaction Reports and Analysis Centre

TERRELL, Mr Kim Christopher, Acting Chief Executive Officer, CrimTrac Agency

WALTERS, Mr Mark, Acting Director, Technical Operations, Australian Federal Police

CHAIR—I declare open this public hearing of the parliamentary Joint Committee on the National Crime Authority in relation to its inquiry into the law enforcement implications of new technology. I welcome our witnesses from agencies within the Attorney-General's portfolio. We have received from the Minister for Justice and Customs, Senator Vanstone, a submission which has already been published by the committee. It is proposed that Ms Ellims will make a brief opening statement, followed by Ms Montano, and then we will go to questioning from the committee. I remind my committee colleagues that, as the witnesses are public servants, the officers should not be asked to give their opinion on matters of policy. They are here to assist the committee to understand relevant policies and administrative processes in relation to the inquiry's terms of reference. You have been advised by the secretary that the committee prefers all evidence to be given in public but that you may at any time request that your evidence, part of your evidence or answers to specific questions be given in camera and the committee will give consideration to any such request. I understand that you have foreshadowed the possibility that you may indeed wish to answer some questions in camera and, as a matter of convenience, we will seek to conduct any in camera session at the conclusion of the public hearing. That said, I invite Ms Ellims to make a statement.

Ms Ellims—The Attorney-General's Department and its portfolio agencies are very pleased to be able to make a contribution to the committee's inquiry into the law enforcement

implications of new technology. The portfolio submission represents a coordinated response to the inquiry's terms of reference on behalf of both the department and relevant portfolio agencies, namely the Australian Transaction Reports and Analysis Centre, AUSTRAC; the Australian Customs Service; the Commonwealth Director of Public Prosecutions; the Australian Federal Police; and the National Crime Authority. The submission also draws on research conducted by the Office of Strategic Crime Assessments, the National Office for the Information Economy and the Australian Institute of Criminology.

The Commonwealth submission recognises the very rapid development of new technology, the most significant area of which has been without doubt the revolution in information technology. More than 3.2 million Australian households now have access to the Internet, reflecting Australia's high take-up rate of new technology, and it is estimated that worldwide, more than 900 million people will be using the Internet by the end of the year. While these developments provide opportunities for industry and commerce, the Commonwealth recognises they also provide new opportunities for criminals and criminal organisations to commit crimes. Electronic technology presents the opportunity for criminals to engage in anonymous activity with jurisdictional complexities which have the potential to frustrate law enforcement.

The range of criminal e-crime activity potentially includes intellectual property theft, denial of service attacks, child pornography, fraud, virus propagation, spamming, the dissemination of offensive materials, commercial espionage, sabotage, electronic terrorism, cyber stalking, extortion, tax evasion and money laundering, and I am sure that that is not an exclusive list. The global reach of such crimes is illustrated by the love bug virus, for example, which is estimated to have infected tens of millions of computers, including systems operated by the CIA, the Pentagon, and the British parliament.

From the Commonwealth's perspective, legislative responses need to be underpinned by stronger links between public and private sector stakeholders, continued exploitation of new crime fighting technologies, improvements in mutual cooperation, resource sharing and national policing information systems, and a balanced approach to community concerns in relation to privacy. The major consideration of the Commonwealth is the need for a sensible balance between encouraging and facilitating the use of new technology in order to strengthen commerce and industry, and simultaneously providing protection for consumers from the potential repercussions of criminal activity.

The portfolio submission also recognises that the e-commerce industry has a vital role to play in ensuring a safe and secure on-line environment. Effective protection from threats within the electronic environment will require resources from industry, in partnership with government and the law enforcement agencies. In particular, the adoption of appropriate risk management and harm minimisation strategies by the private sector will be critical to reducing the incidence of electronic crime. Commonwealth initiatives to assist in implementing these strategies include the Action Group into the Law Enforcement Implications of Electronic Commerce, AGEC, which is chaired by Elizabeth Montano. AGEC facilitates and encourages businesses and consumers to establish an environment hostile to crime.

I would like to take this opportunity this morning to examine some of the key issues that have been raised in the department's submission, and outline the government's law enforcement policies, particularly in relation to the use of computers and electronic communications

technology. The government recognises the great benefits that will flow from the use of technologies. The permeation of electronic commerce through our economy has the potential to create enormous business efficiencies and significantly boost economic growth. Banking, stock exchanges, air traffic control, telephones, electric power and a wide range of other institutions are already largely dependent on information technology for their operation, and the Prime Minister has committed the Commonwealth government to moving all appropriate government services on line by July 2001.

The government has a range of programs and measures designed to promote the uptake of e-commerce in Australia, acknowledging that the adoption of the new technology will be led by industry. Where necessary, the Commonwealth has acted to introduce legislation to provide an environment conducive to e-commerce. The Electronic Transactions Act 1999 is based on the United Nations Commission on International Trade Law Model Law on Electronic Commerce and the recommendations of the Attorney-General's electronic commerce expert group. The act removes pre-existing legal impediments that may prevent a person using electronic communications to satisfy legal obligations under Commonwealth law. The act gives business and the community the option of using electronic communications when dealing with government agencies.

To safeguard individuals' rights to privacy, the Privacy Act 1988 regulates the collection, storage, use, disclosure, access to and correction of personal information by Commonwealth public sector agencies, including law enforcement agencies. The Privacy Amendment (Private Sector) Bill 2000 will implement the national principles for the fair handling of personal information which were developed by the Privacy Commissioner following consultation with business, consumers and other interested groups. It will provide minimum standards for the collection, use, disclosure, security of and access to personal information by private sector organisations.

The portfolio's submission recognises, however, that, as our reliance on computer technology grows, steps must be taken to ensure responsible risk management to preserve trust, confidence and security in electronic commerce. Incidents such as the intrusion into the Australian Taxation Office GST ABN web site through unauthorised hacking highlight the need to avoid complacency in relation to the protection of electronic commerce from criminal activity. As the use of technology to conduct government business online grows, potential exposure to such incidents will be unavoidable.

As technology advances, such electronic crime can be expected to increase in its scope and impact. Dr Peter Grabosky of the Australian Institute of Criminology notes that increasing computer use in connectivity not only increases the number of prospective victims of computer related crime; it also increases the number of prospective offenders. The Office of Strategic Crime Assessments has also identified the potential for increases in crimes of acquisition, such as fraud, and has highlighted the fact that organised crime has the potential to launder the proceeds of criminal activity by electronic means. Such threats of electronic criminal activity raise new challenges for prevention, detection, investigation and prosecution of offenders. Commonwealth strategies to address emerging issues include development, enforcement and administration of criminal law, national coordination of state and territory government responses and international cooperation.

Consistent with the need to keep pace with sometimes rapid development in technology, the portfolio has developed legislation that, as far as possible, is technology neutral. The Commonwealth is concerned that legislation must meet the needs of business to minimise or remove international trade barriers and provide consistent jurisdictional requirements while also protecting consumer interests.

The Model Criminal Code project developed in cooperation with state and territory governments is expected to be completed by the end of this year. The code updated offences such as dealing with unauthorised misuse, alteration or erasure of computer data to bring them into line with new technology. The code also includes sabotage offence provisions which carry a maximum penalty of 25 years imprisonment against terrorists convicted of attacks, including cyber attacks on public facilities such as government offices, public transport and water or power supply systems. The agreement by the states to give these offences priority in 2001 will introduce national coordination and improve consistency of offences throughout Australia.

The Telecommunications (Interception) Amendment Act 2000 has addressed the difficulty of detection imposed by subscribers using several mobile telephone services in the one handset simply by swapping around their subscriber identity module cards. The amended legislation provides for warrants to be issued in relation to any telephone service used by a particular person, enabling law enforcement agencies to intercept any services which are or are likely to be used by the person named in the warrant.

In regard to international cooperation, one of the major difficulties in dealing with the changing nature of crime in the new global electronic environment is specifying the jurisdiction in which an offence occurs and which legislation or regulations apply. The threat of electronic crime presents special challenges for the detection, investigation and prosecution of offenders.

In response to this borderless nature of electronic crime, the government has strengthened the Mutual Assistance in Criminal Matters Act 1987 and continues to negotiate treaties and extradition arrangements with a wide and growing range of countries. Committee members would be aware that the active participation of Commonwealth agencies on international task forces is also contributing to identification of issues of common interest and sharing of crime-fighting techniques.

Australia's international commitment is demonstrated through the government's ongoing support of and cooperation with the activities of international organisations such as the Financial Action Task Force, the World Customs Organisation and the International Organisation of Computer Evidence. The portfolio's submission recognises that further efforts in these areas are essential for future progress in international law enforcement. Of particular importance is the need to develop mechanisms to provide and receive real-time assistance from foreign investigators.

The government remains determined that profit obtained from criminal activity should be confiscated, particularly to prevent the reinvestment of that profit into further illegal acts. Amendments to the Proceeds of Crime Act 1987 to introduce a non-conviction based, or civil confiscation, regime will extend to the recovery of profits gained from unlawful criminal activities such as money laundering or dealing in narcotics.

There are also many new and developing technologies which reduce the opportunity to commit computer related crime, including technologies of encryption and anonymity, which permit concealment of details such as credit card numbers or the identity of the communicator. Passwords, biometric devices such as fingerprint, voice recognition and retinal imaging technologies are also advancing. The government adopts the policy that the first line of defence should be self-defence. Accordingly, the portfolio submission indicates the Commonwealth's support and encouragement for the sharing of awareness and application of such new technologies among law enforcement agencies and the private sector.

I understand the committee may have a particular interest in CrimTrac. I have asked Kim Terrell, who is the Acting Chief Executive Officer of CrimTrac, to come along to answer any questions you might have this morning. The Commonwealth has devoted significant resources to law enforcement issues associated with new technology, and one example is the establishment of CrimTrac. The Commonwealth has put in $50 million over three years to introduce new information technology capabilities for law enforcement through the national CrimTrac system. CrimTrac will provide access to timely, accurate, comprehensive and relevant information essential for effective crime detection and prosecution of offenders. You may have seen the article in the *Australian* over the weekend, which gave a sense of the attitude of some of the law enforcement agencies in the states to CrimTrac. It was a good article.

In conclusion, the challenge which new technology crime presents to law enforcement is a formidable one. The portfolio submission recognises the need for ongoing monitoring and evaluation of Commonwealth legislation in particular to ensure it is relevant to change in new technology and to ensure that the powers of law enforcement agencies are adequate. The submission reflects the Commonwealth's recognition of the particular need for increasing use of new crime fighting technologies and a focus on education, awareness raising, crime prevention and harm minimisation, as well as detection, investigation and prosecution of offenders where new technology is relevant. Of particular importance is the improvement of communications and working relationships between governments, business and law enforcement agencies, both domestically and around the world.

A person who helped me write this found a very interesting quote which I will mention to you. In *The Lost Worlds of 2001*, the British science fiction writer Arthur C Clarke wrote, 'The only way of finding the limits of the possible is by going beyond them into the impossible.' The Commonwealth recognises that innovative responses which go beyond today's horizons are continually going to be needed to maintain pace with the speed of anticipated changes in technology. I can assure you that the government and the law enforcement agencies are committed to addressing this challenge.

CHAIR—Thank you.

Ms Montano—I would like to make two opening statements, the first one as Director of AUSTRAC—the Australian Transaction Reports and Analysis Centre—and then a brief comment in my role as Chair of the Action Group into the Law Enforcement Implications of Electronic Commerce.

AUSTRAC speaks as a regulator and as the specialist financial intelligence agency. The Financial Transaction Reports Act, which is the act through which AUSTRAC undertakes those

two tasks, works to a reasonable degree in the current environment. It leverages off the existing financial sector practices and infrastructure—for example, the international funds transfer instructions we collect are leveraged straight off the SWIFT messaging system, which is the international way in which banks interact with each other in the international payments system. So our work directly leverages off and is totally dependent upon that infrastructure.

New technology and globalisation are going to change all that. There are two main streams to these changes. One is in relation to identification—that as institutions are having more and more difficulty in identifying their customers and when real Internet banking comes in, rather than just saying, 'I'll give my instructions over the Internet'—which is what happens primarily at the moment—there will be quite extreme difficulties in seeing how transactions relate to real people. This is an issue for the private sector as much as for the public sector. In fact, there are enormous commonalities of interest. We are working pretty closely with the financial services industry on that.

The second stream is in relation to the transactions themselves. Systems are vulnerable where our current catchpoints are bypassed or altered so that our traditional strategies do not work any more. AUSTRAC research is showing that, while changes are very slow in some ways, in others change is very fast. While the private sector are very keen to embrace technology, they are in fact business people and as such they do not actually launch products until they are sure they are going to work, so that they fit their risk management profiles as well. We actually do have windows of opportunity to do things, but we have to catch them at exactly the right time.

A lot of our research has been devoted to technologies and practices which perhaps are on the shelf for the moment—for example, smart cards. We were all very concerned about those several years ago and their possibilities for money laundering activities. At the moment, smart cards are, quite clearly, a technology looking for a business case. There are some that are looking for multiple applications, but as soon as those commercial conditions are ripe they will be off and running. While we might take the view in the short term that they are not a problem for law enforcement per se, because we are talking about low value, the moment someone wants to put a lot of value on it—which is only a matter of time, commercially speaking—we will have some significant issues. So that is an example of a technology which has to be watched, but we have to be ready to jump pretty quickly. We cannot wait two or three years while people decide, 'Oh, there's an issue; let's work on it.'

We have got a whole lot of other technologies happening, such as screen scrapers which aggregate information that is available over the Internet. That is an actual value added service that someone gives where you can find out all your financial information. That has some implications now, but they are going to have huge implications when you not only give the aggregators the power to go and get your account records but also start to give them the capability to transact on your behalf. So in the context of a piece of legislation like the Financial Transaction Reports Act, there are an enormous number of issues to deal with. The challenge, of course, is to get our timing right and to make sure that the changes that are made are going to stand the test of time through things that we researched and drew conclusions about two years ago, which are now out of date. So the normal programs have to be adapted. We have to go back to basics. From an anti-money laundering point of view, anything which allows value to flow out and around Australia without an audit trail which can be followed by law enforcement agencies, when necessary, is a danger and it is one which we have to manage.

On behalf of the AGEC, I would like to make an opening statement. The Action Group into the Law Enforcement Implications of Electronic Commerce was formerly known as the Research Group into the Law Enforcement Implications of Electronic Commerce. The reason for the name change is that we were told that we should be acting rather than researching, so we are trying to do that. It has representatives from most of the HOCOLEA on it. As you can see, it is a very cross-portfolio oriented approach. Some of the issues that are relevant to ASIC, for example, are totally relevant to the AFP and the NCA. While they might be investigating different kinds of crimes and in different jurisdictions, the reality is that the techniques and the infrastructure that criminals will be relying upon is the same. So when the agencies go in, they are the same issues they have to deal with.

We also have on the AGEC, the Australian Centre for Policing Research in order to get the state and territory perspective. We work very closely with them in relation to where we think the boundaries are blurring between community policing, state and territory issues as opposed to national issues. What we have been trying to do is explore the implications of electronic commerce and the wider information economy for law enforcement agencies and revenue agencies. As you know, we have produced a report. We are currently working on the recommendations to that report through an action plan. We are trying to work on both the environmental issues and the tools and powers that will be needed by those agencies when they are expected to do their jobs in new environments.

CHAIR—Thank you very much. I am going to pass up the chairman's usual prerogative of firing the first question because Senator Ferris has to leave us at 11 o'clock. Therefore, I thought I would give her the first question today.

Senator FERRIS—Thank you very much, Chair, I appreciate that. Ms Montano, as you would probably remember, I have visited your agency twice now and I have quite a longstanding interest in it. Could you tell us about what you described as really quite challenging changes that have occurred in the area where AUSTRAC operates. When we first came as a committee to see your operation I remember being extremely impressed with the way you were able to intercept, but $10,000 does not seem to be very much any more. Is that still a reasonable limit? Are those very impressive operations that you had three years ago still working as well as they were then, or do we need to have another look as technology has changed so fundamentally since then? There are a few questions bound up there but they all really come into the same area.

Ms Montano—The limit of $10,000 in relation to cash transaction reporting is still a reasonable limit. It is still reasonable in the sense that for many crimes the real issue is how you get the street proceeds into the financial system, and $10,000 is still a reasonable figure. It is a still a reasonable sum in the sense of trying to exclude lots of ordinary commercial and private transactions which should not be the business of an agency that looks at serious money laundering. It is not a bad threshold for cash. The areas of vulnerability are in relation to the electronic transfers.

As to how well it is going at present, it is still producing lots of very interesting information which is of great value to investigating agencies. We are in a period where we have some really great opportunities to think about the future and to think about value movement in new ways, and that is what we are trying to do now. It is fine for now, but we need to work now so it is

relevant in three, four or five years time. That is an historical thing. When the FTR Act was first thought of, this was quite revolutionary stuff. And in many ways it still is. The approach is still revolutionary, but the financial system that we leverage off is changing. The question is how we realign ourselves to deal with proprietary systems that banks give their customers to use so that in some cases they bypass the Australian operations of the banks, so we have some jurisdictional issues. How do we make sure that banks and other cash dealers under our legislation are still able to identify unusual transactions, the suspicious ones? If things are happening electronically, is there a person there who sees a transaction or a pattern of transactions and says, 'I think this is odd. I want to report it as suspicious'? There are those sorts of things. That is what we have been working on pretty hard for the last few years.

Senator FERRIS—Are the banks as cooperative as you would like them to be?

Ms Montano—They have some real dilemmas in knowing what to say when we go and talk to them about new technologies. They are all in a very interesting situation. They all want to use these new technologies, they all want to get the market advantage, but they are also people who have to manage their risks. So often they have got a lot of risks to deal with, internally, before they get to the point of launching a product. They are often quite guarded about talking about them. They are often, when we go and talk to them, still thinking about them themselves. Often when we go and talk to them about a product it will be almost too early in the process. Then it will happen very quickly and when we come in it may well be too late in the sense of trying to influence the creation of the product. We could certainly do a lot more work in relation to the research and development angles of what are the products that are being developed. Often they will be germinating in the minds for quite a long time and then a competitor will hit the market and they will rush out a product within weeks to try and get some market share. So they are moving very fast, often after quite a lot of procrastination about the general issues. It is hard to pick them sometimes.

Senator FERRIS—What about things like underground banking, stored value cards, that sort of thing, where, as you say, nobody ever sees the transaction, the whole lot is done electronically? It might be done from the privacy of somebody's home by opening an account on the net so that there is no evidence that the money is deposited in Australia. Are banks interested in that issue?

Ms Montano—Banks are very interested in anyone who takes business away from them. Underground banking is very interesting. There are some remittance dealers who basically operate as underground bankers in the sense that they are providing alternative kinds of systems to banks. Obviously the institutions do not like that. It uses their infrastructure, because the remittance dealers are customers, but of course the cream off the top is actually going to the remittance dealers, not to the institutions.

But there are other kinds of underground bankers who very rarely use the financial system. Some of the ethnic underground bankers, in fact, just run sets of books which are basically set-off accounts. They will actually set-off with a counterpart in another country once every few months, once in a blue moon, so that a whole lot of transactions will happen and you will just see one big global set-off at the end of a period. Those things are not actually conducive to the sort of analytical work we do. Having said that, when you have other intelligent sources that tell

you what is going on, the combination of sources is still useful, but it is an area where it is difficult to automatically pick up issues.

Underground bankers will always be an issue. They are an issue in all societies. Often underground bankers are not doing anything nefarious; it is just a cultural way of dealing in value, particularly for people who come from countries where they do not trust the stability of the institutions or their political processes and they have to trust the people they really do trust to move their money around. Underground bankers are very complicated. We are actually doing a fair bit of research work on that under the National Illicit Drugs Strategy, and we have identified quite a few additional cash dealers who are being enlightened as to their obligations to report under the FTR act. I think we are at a point in time where, while everything is pretty effective at the moment, there are some big changes coming, and the sooner we are ready to jump in, the better.

Senator FERRIS—Are banks as tough as you would like them to be on false identities? It is very hard for us to run around and pull 100 points together, but it is incredibly easy for somebody who is dealing in that every day. Are banks as tough as they could be on false identities and checking identities?

Ms Montano—I think they are becoming far more tough about it, but that is self-interest as much as anything else. The FTR act was introduced 10 years ago or so, and even in a Senate committee hearing in 1993 the Australian Bankers Association objected to the costs of identifying their customers, as imposed by the FTR act. It is very interesting that seven years later the tune is that they are not doing enough to identify their customers, on the basis that there is such a large amount of fraud happening, much of it based upon false ID. So the banks have a lot of self-interest in doing it. At the same time, they have some problems—as do, for example, the Internet gambling organisations—in identifying who they are dealing with sometimes. Sometimes what is enough for their commercial purposes will not be enough from a law enforcement perspective. So if you have a valid credit card and someone is going to do something, you may well think, 'That is sufficient identity for our purposes; we have managed our risks,' but obviously from a law enforcement and government perspective, that is not a sufficient identifier. The banks, in particular, are very concerned about that. They have had a lot of fraud, a lot of it based on false documentation which is counterfeit or improperly obtained genuine documents. So, yes, they are very concerned. We are actually working with them in an identity steering group.

Senator FERRIS—What about the role that law enforcement might play in the same sort of area? For example, I think this committee in the past has often been surprised at the extent to which the police agencies in various states have not embraced the need to train their officers in some of this new technology. Do you work very closely with police agencies on an interaction of skill basis rather than simply on the law enforcement side of cash transactions?

Ms Montano—Something the AGEC has been working on is that issue of training people. If the reality of life is that the skills we are talking about are equally attractive to private sector and public sector employers—and the private sector is often going to win out in terms of the remuneration you can offer—then the public sector has to develop other strategies. The public sector has to give people who are the 'techos' career paths rather than seeing them as being specialists in the corner. It obviously has to take the view that there are some things the public

sector just cannot do, and it will have to enter into arrangements with the private sector to do a lot of work. A number of agencies do that already, they have a lot of their leg work done by private sector organisations, and that may well be a reality they will have to get used to. And more to the point, it is very hard to stay technically at the front if you are someone who only does training every few years. It is a big investment to make and, of course, that makes you very attractive to the private sector.

Senator FERRIS—The NCA has been able to bring in specialists when they have needed to, particularly from the accounting profession; but it is a little more difficult for a state based police agency, isn't it?

Ms Montano—I am not sure if it is any more difficult for them, in the sense that, if they have investigations that need certain kinds of computer forensic skills and they can enter into arrangement with the private sector to provide those skills and there are appropriate checks and balances, then it is certainly a strategy which has to be looked at.

CHAIR—Can I just take that one step further. What sort of work do you do with the other end? In other words, not just what is going on in Australia but obviously the very essence of what you do is international. What sort of cooperation do you get overseas? You might like to give us an idea of some of the generic measures you take but perhaps also gives us an indication of which countries are cooperative and helpful and supportive and where you might have particular difficulties.

Ms Montano—There are two aspects to that. One is the practical cooperative measures. From AUSTRAC's perspective, we have agreements with seven other countries to exchange financial intelligence. We would like a lot more but we have to ensure reciprocity; we have to ensure that the information we provide will be dealt with confidentially. As a matter of policy, it is a question of whether there is enough trust between the two counterparts. We are looking for more and more parties to enter into those agreements with. You have to take the view that you have to go for the ones that are most strategically important to you. They are the ones you go to first. We have agreements with the UK, US, New Zealand, France, Belgium and Denmark; and it is really an issue of some technology exchange in some particular instances. The Minister for Justice and Customs has just signed one with Italy, because there are a lot of flows backwards and forwards and some technology issues as well. We have other ones in the pipeline.

We are probably experiencing what a lot of law enforcement agencies are experiencing around the world: having had certain kinds of domestic and national approaches to things, seeing how they actually mesh with the domestic and national programs of other countries, and whether the way in which we think about the exchange of information and the circumstances in which we will do it are the same as they will do it. A lot of the ones we are still negotiating in fact go straight to that point: how do we exchange information, in what circumstances? How can we streamline it better? At the moment, the exchange of financial intelligence under the FTR act is dealt with as a kind of mutual assistance, and that may be something that we need to change on the basis that it is not the way a lot of countries in the world are going. That reflects the fact that we were actually one of the first to do that sort of thing and it was thought of being a mutual assistance type of thing. A lot of other countries, particularly ones that work very closely in Europe, are far more interactive with each other about that. While historically we have not had to be, we will have to be in the future.

The other level on which we interact is in the various international fora. The Financial Action Task Force, which was mentioned in the opening address by the portfolio, has as one of its 40 recommendations to encourage countries to look at the risks behind electronic commerce. We were actually one of the drivers for that recommendation to go in. Australia is probably one of the most advanced in terms of doing the sort of research we are talking about. In terms of particular countries, we interact a lot with the United States and with the United Kingdom in relation to this sort of area. The US is very advanced in some of its legislative provisions and in some of its capability mechanisms. The UK has been going through a big process during the last couple of years, and we have been having discussions with NCIS—the National Criminal Intelligence Service—which is our counterpart in the United Kingdom It has a much wider role than AUSTRAC but, in terms of financial analysis, it is our counterpart.

For a lot of countries, it is an issue on which there is a lot of talk but there is not necessarily a lot of action yet, in the sense of trying to work out exactly what you put in place to deal with this. So I think a lot of countries are still in the exploratory phase. Many countries are going to make the really big leap from financial systems which rely a lot on cash to the Internet and other kinds of electronic transactions when they have not actually done the intermediate step, as Australia and some others have done, with cheques, direct debits and all those sorts of things. Their societies are actually going to make the big move from cash oriented to electronic transactions very quickly. So their approach to this is very different. Many of them still think that cash is a really big issue—and it is. It is still a big part but it is not the big driver for us as much as it used to be. We are having a lot of those sorts of discussions with other countries where we say that we are doing this, this and this, and ask, 'What are you doing?' I think they are still emerging issues for a lot of them.

CHAIR—The countries that you have named where we are doing predominantly that cooperation are what you might loosely call OECD type countries. As I understand it, a lot of money laundering presumably comes out of drugs and a lot of the drugs come from Asia. If that is not correct, please correct me. But I would have thought that we would get a lot of drugs coming in from Asia and presumably there is money wanting to go back there. What are we doing with Asia? I was in Singapore a couple of weeks ago talking to their national drugs group. They were interested in what you are doing and, as I understand it, want to go down a similar track. They are very much a First World economy with a substantial banking system. Could you give us some outline as to what we are doing in this region of the world?

Senator FERRIS—And also South America. I do not think you mentioned any South American countries either.

Ms Montano—First of all, in Asia, two of the jurisdictions that we are negotiating with in relation to new MOUs are Singapore and Hong Kong, China. The links are very much there and we hope that there will be others. Because we try to work on a reciprocal basis, obviously one of the issues about getting some international cooperation is to encourage other countries to have systems similar to ours. Australia has had a very major role—in fact, it has been the lead country—in establishing the Asia-Pacific Group on Money Laundering, which is a regional FATF star body and is supported by the FATF on the basis that there are some particular regional issues in a whole lot of different regions and it is better for them to have regional groupings. We are very active in pursuing that. For example, in the Asia-Pacific context, we are in the middle of a mutual evaluation process where we look at the anti-money laundering

programs of all those countries. We were a member of an evaluation team on Vanuatu earlier this year and have done a lot of work with Vanuatu in encouraging them to develop really good anti-money laundering laws and systems. That is progressing very nicely.

Yes, there is work to be done in the region. In many of those countries the societies are very cash oriented. For example, they come and visit us and talk about setting up systems like ours and we start talking about cash reporting. When we talk about the fact that we have a threshold of $10,000 for our cash reports, I always preface my comment with 'That is an appropriate monetary limit for what might be unusual in the Australian context because Australians do not, as a rule, carry around lots of cash.' But in some of those societies cash is the way of life. When some of these people walk around with large amounts of cash that is not an indicator of suspicion at all. It is normal behaviour, both commercially and personally. So you really do have to pick the right threshold. That is what I meant when I said that some of those countries are very cash oriented. It will be very interesting to see how some of those people make the transition from cash to electronic transactions.

Senator Ferris mentioned South America. Three South American countries—Mexico, Brazil and Argentina—have just been admitted to membership of the FATF in the last 12 months. It is the first time that membership has been opened in 10 years. These countries had to go through a mutual evaluation process and had to get their anti-money laundering programs up and running. They have a South American regional grouping where they are working on exactly the same issues and they have a lot of interaction with the US. The theory is that you will have a series of these regional groupings around the world that will foster national environments which will then be conducive to international cooperation. With some countries you try to get them to build the foundations and then you can interact. That is a process that you have to work on from a number of perspectives—one, on the straight regulatory issues and, two, on what can be leveraged off that in terms of law enforcement cooperation. The Africans have a group that has just been formed under the auspices of the Commonwealth Secretariat. The UK is a big supporter of that. It is set up and based in Tanzania. There are a whole lot of these regional groupings forming.

CHAIR—I should not hog the questioning. Mr Edwards, do you have any questions?

Mr EDWARDS—I would like to ask Ms Ellims a question. I think you said that there are about to be nine million people on the Internet in Australia. Of that nine million, can those people be confident in the security of the personal credit card information they provide when they are entering into transactions?

Ms Ellims—I think the short answer is variously. What I said was—just to make sure the figures are right—more than 3.2 million Australian households have access to the Internet now. It is a high take-up; Australia is quite high in that regard. Worldwide, more than 900 million people will be using the Internet by the end of this year. There are a number of ways of looking at this. One way is from the point of view of crime prevention. Ms Montano might want to comment on this. Certainly, from the Commonwealth's point of view, a major policy is to encourage industry, the private sector, to develop all the crime prevention mechanisms that they can in order to ameliorate the possibility of fraud committed over the Internet. The Commonwealth encourages the private sector to use the range of technologies that are available in order to avoid the creation of a problem.

In terms of what law enforcement can do, Ms Montano may wish to comment and also the AFP representative, Mark Walters, whom I did not mention at the outset. He is available here to comment if the committee would like to hear from him. The reason the AFP may be worth hearing from is that they are leading, from the Commonwealth point of view, a major initiative in regard to e-commerce with other police commissioners in the states and territories. Elizabeth, do you want to make any remarks about that and then perhaps the AFP?

Ms Montano—Yes. One of the major impediments to a really widespread take-up of commerce on the Internet, as we all know, is the security issue. The private sector has enormous amounts at stake in terms of making sure that credit card details are safe. So, of course, we have encryption being a standard in relation to the transmission of credit card details. Often you have a message with the unencrypted part—for example, 'I would like to buy a pair of pants'—and then the encrypted part will be your actual credit card numbering. So there are a lot of private sector mechanisms and really it is a job for them. I mean, it is target hardening in the old law enforcement parlance. It is making sure that it is as robust as it can be. Apart from that, having reduced the possibilities, you then get back to the normal issues—for instance, what can law enforcement agencies do after the crime? That is to say that they need to be able to trace these things, to get the records and find out who has done what, where and when, and investigate in the way in which they would investigate a fraud or other kind of crime in the ordinary environment.

Senator DENMAN—If security of the credit card is breached when you are buying pants and so on, whose responsibility is it to bear the loss—the person who has got the credit card or the agency they are buying from?

Ms Montano—It is usually dealt with by contract. Often, as a feature of pure marketing and promotion of activity on the Internet, the credit card providers will do that. They take the risk in relation to stolen cards. For example, there are a lot of sites where services are provided in exchange for credit card payment, where the credit card holders then deny the service was theirs—so it goes back to the provider. But that is a commercial risk that credit card providers make. It is like having your credit card skimmed twice at a restaurant and someone taking off. As a matter of commercial reality, the credit card provider who is trying to encourage people to use their cards and not be afraid will take the risk. The interesting issue is, when does that risk get big enough that they are no longer prepared to take it and so they want to put the risk back on the customer? That is a really big issue at the moment.

For example, AMEX has decided that they are not going to provide their cards to certain kinds of sites on the basis that the repudiation element from the cardholders is just getting bigger and it is not commercially viable any more. So there are those issues but, at the end of the day, that is just shifting the risk around. In a way, the issue has been masked for a very long time. It is like all bad debts—banks are willing to wear bad debts in relation to fraud when they run at two or three per cent, but when they get much bigger that is when they start to think, 'Now we have to work on another strategy to deal with this.' So all those risk management issues when they are small are pushed to the side in terms of how you deal with them at the base level until they get to a point where someone cannot bear the risk any more and then they have to find new strategies.

Mr EDWARDS—Could we get a comment from the AFP on that question?

Mr Walters—The AFP will be appearing before the committee early in the new year in relation to our submission. That is something that we can address in greater detail at that time. Following on from what Ms Montano said earlier on, it is certainly an issue in relation to working closer with industry in this area. The AFP can respond as other law enforcement agencies can where these issues are breached, but there is certainly a great emphasis on law enforcement interacting with industry to ensure that these security arrangements are in place.

Mr EDWARDS—I assume that the answer we then should be giving constituents who may be shopping before Christmas is that they should use their credit card on the Internet with caution.

Ms Ellims—I certainly think they should investigate the probity and propriety of the organisation with which they are contracting in the use of their credit card.

Ms Montano—It is like dealing with anyone. The basic principle at common law 200 years ago was 'caveat emptor'—buyer beware. Then you have a series of pieces of legislation and market behaviour which modify that in the sense of legal redress. When you go onto the Internet, if you are dealing with one of the major retailers in their online operations, you may take a view that, because of the commercial circumstances, you are far more comfortable in dealing with them, that the credit card provider will take the risk. You might take the view that, all things being equal, that is not a bad way to do it if you want to avoid the Christmas rush in the shops. But if you are buying—I will not name a country—

CHAIR—Why not?

Ms Montano—No. I am just going to pick a country out of the air and it is not based on any research. That would not be fair. If you want to buy the man who has everything some exotic bongo drums from country X, and you are going to deal with the National Bongo Drum Company of country X, perhaps you would want to think about it. But you would do that whether you were faxing off your instructions with your credit card details on it, or if you were posting them a letter by slow mail, or you were visiting country X, in terms of whether you were actually getting what they said was in the box when you walk out of the shop. They are all risk management issues that consumers have to deal with. So the answer is, if it all looks fine otherwise—

CHAIR—But the difficulty is that, unless it is a company that you know in some other context, isn't it the case that on the Internet it is far more difficult to discern whether they are a substantial and reasonable operation—because what you see on your screen can look just as valid if it is a one-man band with a $2 company as effectively as a billion dollar company that has got huge resources and staffing and credibility and all the rest of it.

Ms Ellims—That is true. What Elizabeth said about checking the probity and propriety of any company of course still remains. If you are choosing to buy off the Internet, quite often you will know the company—just as, if you are choosing to buy through mail order, you will either know the company well or not so well, in which case you will need to do some other checks. One thing I should mention here is that the National Office for the Information Economy has produced a publication in the last month or so which sets out the Commonwealth's position in relation to purchasing off the Internet, particularly in relation to Christmas. We are expecting it

to be a potentially high volume transaction time. That little booklet is actually quite useful in terms of setting out the sorts of things that a consumer might wish to do in the process of purchasing through the Internet. That is certainly worth looking at from the point of view of effective transactions and protecting oneself—harm minimisation.

CHAIR—Whilst we are talking about the Internet, do you have any comment on the FBI Carnivore system?

Mr Walters—Yes, I have heard of that system but I am not personally familiar with it. That is something that the AFP can address to the committee when we appear—

CHAIR—It is my understanding that they have basically got an Internet tapping system which runs a sort of packet-sniffer program to collect data from various ISPs and things like that. I suppose the question is not only are we interested in whether you have got any views on its effectiveness, but if you have got views that it is effective, we would be interested because the government might want to go down the same line. So if you are not aware of that, perhaps you could take that on notice.

Mr EDWARDS—I just wanted to raise that particular issue to try to bring it down to the level of the ordinary Australian, but I now want to turn to a more global issue. You point out in your submission that in Australia we can, for example, apply for a search warrant to support a foreign investigation or apply for a production order. However, Australian law enforcement officers cannot apply for a telecommunications interception warrant or listening device warrant to support a foreign investigation. Given what we have been talking about this morning in terms of the need to be right on the spot, how much of a problem is that? And is that something that we should be looking at as a priority?

Ms Ellims—I will ask Peter Treyde to address that question.

Mr Treyde—You are right in saying that the Telecommunications (Interception) Act does not presently provide for the passing of information that has been gained through telecommunications interception on to agencies from other countries. At this stage it is not an issue that I am aware we have had call to consider from a policy perspective; so there has been no work that I am aware of done in the department on that particular issue.

Ms Ellims—Mark and Elizabeth, you may wish to comment.

Mr Walters—I am not aware of any work that has been done in relation to that.

Mr EDWARDS—I was really asking whether it is a problem that we do not have the ability to do that.

Ms Montano—It is.

Mr EDWARDS—Is it a problem?

Mr Gray—From the DPP's perspective, as the end user of the material that comes through, one of the things we are doing through the action group on electronic commerce is putting together a series of issues papers, and this is the one I am sort of half way through. It has not been a problem to date, and I have been thinking why that is. One reason is the narrow range of offences that you can get TI warrants for. The other one is the nature of mutual assistance: it tends not to be real time, it tends to be something done after the event, whereas telecommunications interception is a real-time investigation tool. So you cannot, at this stage, build a case based on past experience to say, 'It is very important that we should have these tools to support foreign investigations.

But the big 'but' is the fundamental principle that investigative tools which are available to support Australian investigations should be available to support foreign investigations. That needs to be written into general legislation somewhere because there are a whole lot of things. We have not yet identified all of them but we will work through them all in the course of this AGEC exercise. There are a lot of things which cannot be done for foreign investigations which can be done in Australia. I just think that is not the way to approach investigations in this area.

The other thing that we are likely to see, and another thing that will come out of this AGEC exercise, is pressing to have the range of offences widened. The general concept is that if people commit offences electronically then you should be able to go into the electronic medium to investigate them, but the list of offences under the Telecommunications (Interception) Act do not allow you to do that at the moment. So it is sort of the chicken and the egg. What do you do first? Do you widen the offences in the TI act and then say we need them to support foreign investigations, or do you get TI warrants for foreign investigations and then look at the sort of case you use them in?

The other factor why it has not been a problem is the resources that are required to monitor telephones. The capacity is increasing, but until fairly recently the number of telephone services that could be monitored at any one time were very limited. I really think the Australian agencies would not welcome the suggestion they should devote those scarce resources to supporting foreign investigations. It is an emerging issue, and how that fits into the order of priorities is really a matter for the committee and the policy makers.

Ms Montano—That particular issue is one of a much bigger picture. If you look at the whole structure of the criminal law, it is all based upon the particular environment it works in. It is only when you think about the different dynamics of a new environment that you work out why some things need changing. It is not that the legislation or any of these things are sort of historically deficient, no-one needs to be on the back foot about that, it is just that they worked in a certain environment in certain sorts of circumstances, but they may not be the total answer in new environments. And while the principles underlying them will be the same, you do have to expand your horizons. Although you do not have any cases you can point to that have failed because you have not had this thing, you know that when these new things happen, these are the sorts of things you are going to have to have in place to make it all work.

When we talk in our report about the history of law, case law was developed as real things happened in the real world, and that is the way judge-made law works and it is the way that legislation has worked. You would never put in a piece of legislation unless you have cases and research to show that society needs this thing because certain things have happened or not

happened in the past. What we are talking about is trying to get ourselves ready for a future where we are not actually sure sometimes exactly what is going to happen. But if you draft things generically and you draft things in a way that can adapt to particular situations, then you will be able to work with it. Having said that, you have always got to be careful you do not draft things so widely that they have unintended consequences. It is a real balancing issue, but the more we can find out what we think the future is going to be like, the better we will be prepared, because it is all moving so fast.

Mr EDWARDS—I take the point. I do not think anyone needs to be on the back foot either. But from our point of view, being interested in legislation and in how we get on the front foot, and given the portability and the degree with which criminals are accessing all of these things, it just seems to me that we are constantly coming from behind. I do not think anyone needs to be on the back foot, but it is certainly helpful to us as a committee if you can try and put us on the front foot.

Ms Ellims—I can make a general comment about that. From a policy point of view, prevention is even more important in this area than perhaps in others, because it is such a rapidly changing world that the best protection for the community generally is to be protected from criminal activity rather than to have to wait for the catch-up, which inevitably will be the case with law enforcement. That is not to decry the importance of law enforcement—it is obviously important in its deterrent effect as well as in catching people who are doing the wrong thing. But the real protection for the community in this area will be in the area of prevention.

Mr EDWARDS—I want to pick up an important issue that was raised by Senator Ferris. It relates to the ability of law enforcement agencies or state jurisdictions to pick up the expertise that is required to try to keep pace with e-crime. It seems to me that, particularly in relation to state jurisdictions, that ability is not there. Can you reassure us that the ability is there within the federal agencies? And are we doing enough to headhunt and recruit the sorts of people we do require to keep pace with and, if possible, stay in front of e-crime?

Ms Ellims—Elizabeth has mentioned that it is a challenge.

CHAIR—That word ‘challenge’ appears in your submission on a number of occasions.

Ms Ellims—I guess that is the reality. Again, it is a function of a fast moving world in the area of new technology, whether it is in relation to information technology or the sorts of things that CrimTrac deal with, that inevitably there will be challenges. The positive aspect of using the word, though, is that we are not seeing these things as irresolvable problems; we are seeing them more as challenges that warrant, and are, being dealt with. It might be best if the agencies comment in relation to that question. They are the ones in the frontline in terms of recruiting and retaining staff.

Mr Walters—The AFP have in place a number of electronic evidence teams to deal particularly with the e-crime environment, and we are trying to maintain and increase their capacity in terms of staffing as well as equipment. Obviously it is a very dynamic environment, change is happening at a very rapid pace and we have to respond to that. Within the organisation we are looking at upskilling all of our investigators to be able to investigate these sorts of

activities, so we are looking at an education program in the coming years to increase our capacity along those lines.

Mr EDWARDS—Although I appreciate your answer, the question was not so much about upskilling investigators; it was more about being able to pull into investigations, on either a part-time or full-time basis, the sort of expertise that is out there in the community. It seems to me that, when you have limited resources, it must be difficult to try to attract the sort of people that you require into agencies to deal with e-crime when there are so many attractive options for people.

Ms Ellims—Which is where purchasing expertise becomes very relevant. That is the reality, I think. Obviously the agencies seek to employ people who are relevant to investigations and upskill those they have, but expertise has to be purchased when that becomes necessary. The Australian Customs Service may wish to comment on this.

Mr Naylor—Certainly it is true to say that we are having difficulty, as are other agencies, in terms of the availability of computer forensic skills, if you would like to call them that generically. We currently use the electronic evidence teams of the AFP for the purposes of our investigations and, in terms of the education program that Mark mentioned, we are talking closely with the AFP to upskill our current investigators—and the point you make I take on board—to be able to better handle the acquisition of evidence from electronic sources in the course of our investigations.

In terms of the availability of expertise and the recruitment of that expertise, we are suffering from the same problems as other agencies: the attractiveness of remuneration in the private sector is somewhat greater than that which we can offer. But it is also fair to say that there are certain companies in the private sector which are offering an outsourced service. We can buy that expertise from agencies who visit us from time to time and offer those services. So far, we have not been so pressed that we have needed that, because we have great collaboration with the AFP, but that is certainly something that we will be looking at closely in the future, because the demand for such service is increasing and the supply is not increasing commensurately.

Senator DENMAN—Can you second from other agencies to your agency for a particular purpose?

Mr Naylor—Yes, we could, but the demand that we have in Investigations in Customs is met, I am pleased to say, by the AFP electronic evidence teams.

Senator DENMAN—So if you had to go to the private sector and use some of their skills on a paid basis, would there be problems? Obviously you would have to do something about confidentiality, which is what I am getting at here.

Mr Naylor—There would have to be a contractual arrangement that would ensure that and, obviously, continuity of evidence and the appearances as witnesses before the court and so forth. Quite a complex contract would have to be drawn up.

Mr Gray—I suppose it is a bit Ludditish, but I really think there are great limits to the extent to which you can bring in those private sector skills. From my point of view, I would much

prefer to see it remain within the AFP. People speak in glowing terms about contracts, but I just do not see how you can prevent leakage of confidential information. It is very much a second-best option, in my opinion.

CHAIR—Isn't one of the difficulties that, when you start to get quantum leaps in technology, upgrading people's skills has its limits, I would have thought. You just get to the stage, as technology develops, that, more and more, those who have been around for a long time—even in the technology business itself—struggle to keep up. It is the younger, quicker minds, I have to say—regrettably. Before I came to this place, I was in the IT industry. There is no question, there are people operating in the IT industry that would just leave me absolutely for dead these days. It is just a different concept in whole areas. It does not matter how experienced you are, it seems to me that there comes a point where a new level of technology comes along where you have got to get some new expertise. Would that be a fair comment?

Ms Montano—Yes, that is right, but there are models in the public sector for having your cake and eating it too in the sense that—

CHAIR—Tell me.

Ms Montano—AUSTRAC is an example. AUSTRAC was set up on the basis that its IT would be outsourced, but outsourced under control. So it is not the 'you give me a service and I don't know how it is done' sort of outsourcing. The IT contractors are under the direct control of the director and go through all the normal security and other controls that one would have in relation to anyone working in the organisation.

They come in. Some of them have been there for a number of years but they are on contract, and they are paid commercial rates. They might do a particular job, developing a particular new software application where, for example, we compete with the private sector for people doing electronic commerce type applications, where the front-end of some of the applications we are developing in relation to getting reports from the cash dealers has exactly the same kind of skills used in web shopping. We compete with the private sector for those people and we pay market rates. They come in, they do a job and they leave.

Obviously, when you are trying to make sure you have got some expertise retained in organisations and you have corporate memories, you have a balance between those people who come in to do particular things, and longer serving people who are in there being your strategists and your architectural advisers and so forth. You also have a few people in-house who know whether you are being conned or not. So there are models that you can develop where you do actually get the best people, but you have to pay for that. At the end of the day, whether you have people within an agency, or sworn AFP officers, or people who float in or out, if somewhere else in the market they are going to get more money and money is their driver, as opposed to career and whatever, then you have got to compete.

CHAIR—Is it always money, or is it sometimes the challenge?

Ms Montano—No, I do not think it is. One of the things I mentioned earlier was, in fact, career paths for the technologists—and that is, again, an evolution of all these organisations. Historically, the people with those sorts of technical skills were the specialists in the corner. If,

in fact, the world is changing and the really strategically important investigations are going to be ones where those sorts of skills are needed, then they are the people you are going to look to for your leaders and your line managers rather than the 'boffin in the corner' role. It is about making life more attractive, and a lot of the people who are out there in the private sector who have gone from the public sector will say that it is not just money, often; but it is, 'Where was I going? What could I build?' So it is a question of cultural changes in those organisations: 'Can I be a leader and be a techo?' If the answer is no, perhaps you have to go to an organisation which will allow you to be that.

CHAIR—Mr Terrell, do you want to add to that?

Mr Terrell—From my point of view I would not like to talk about the conduct of investigations—that does not really belong in the CrimTrac agency's point of view—but in terms of what Ms Montano has just been talking about as far as procuring expertise goes, I would like to back her up 100 per cent. There are many models in terms of being able to bring in people with relevant expertise, and the IT industry is very open and flexible in terms of how you might want to bring in experts to wherever it would be, to develop specific applications and to do things like change management.

You could contemplate hiring people who have particular expertise in strategic planning or designing systems and talking to you about how you should run those systems. The key is that you do have to maintain a balance. You can maintain that balance by having your in-house expertise, and there are public servants who are very motivated and very technically skilled—we have a few of them working for us as well—who can assist you in making sure that the advice you are getting from the private sector is good advice. You can also hire the private sector to provide advice on the private sector. So there are different models that you can look at.

CHAIR—They are called 'consultants', aren't they?

Mr Terrell—I think from the CrimTrac agency's point of view in terms of designing and building major new national systems, we could not do that in-house; we would not pretend to be able to do that in-house; it will take us years to do that in-house. We need to develop those partnerships, and they have to be strategic partnerships.

Mr EDWARDS—I now turn to your conclusion of chapter 4, where you say that while many initiatives are already under way to strengthen cooperative international effort against e-crime 'more progress is required'. I think that is true. But can you tell me how we are, nationally? How are we working between individual state jurisdictions and other agencies? Have we reached a level of cooperation which is as good as it is going to get, or have we got a way to go yet?

Ms Ellims—You are talking about within Australia?

Mr EDWARDS—Yes.

Ms Ellims—There is a series of cascading mechanisms, as you may be aware, arising from ministerial councils—the attorneys-general ministerial council as well as the Police Ministers Council. There are a couple of interesting initiatives arising from both the attorneys-general

council and the Police Ministers Council. Police commissioners, for example, have a comprehensive exercise going on in relation to e-commerce. They have produced a public scoping paper—I am not sure if the committee has seen that—and that is the first step in a major exercise of cooperation among police commissioners, who will be reporting—and do report—to APMC as often as APMC meets in relation to that exercise. There is also a working party arising from the attorneys-general council.

Mr Alderson—In terms of the actual legislation and getting everyone together to have a clear picture on the importance of uniformity between states, a dedicated group of experts has been set up that is under the auspices of the Standing Committee of Attorneys-General, the Police Ministers Council and the National Crime Authority Intergovernmental Committee. It is chaired by an officer of our department, and the other members are three officers from state attorneys-general departments and three officers from state police departments, so that they can get together and get a sense of priorities for reform of law enforcement legislation and start talking about different jurisdictions' interests, so that the focus on uniformity and consistency comes in at the start.

Ms Ellims—The Model Criminal Code exercise is another example of cooperation between jurisdictions. You may have seen the paper in relation to computer crime which was published earlier this year, which is a very significant outcome from that work. So there is a range of initiatives, and these are examples, and it is probably true to say that the extent of cooperation among jurisdictions—whether it is higher than it has ever been, I cannot comment—is extremely high.

CHAIR—We have in the public gallery now a parliamentary delegation from Vietnam, who I met last week in my capacity as chair of the Joint Standing Committee on Foreign Affairs, Defence and Trade. I explained at length the committee system to them. I welcome you, gentlemen, to a public hearing of one of the committees. Please continue, Mr Edwards.

Mr EDWARDS—It is a matter of particular interest of mine, because I wonder how we can keep pace with e-crime when law enforcement agencies in Australia are so fragmented. I wonder if we could go back to the international initiatives. What forums, conferences or processes are there that enable you to strengthen our international ties? How do you go about that?

Mr Hodges—Certainly, Australia is keen to learn from the experience of what is going on in Europe. There are a number of organisations there who have been looking at this issue for much longer than we have. Ms Montano mentioned the FATF initiatives under the G8. There is also the OECD and there are also several UN committees looking at these initiatives. As we said in the submission, the speed of international commerce means the jurisdictional boundaries are crossed very quickly. The criminal elements, of course, do not have problems crossing the international boundaries; the law enforcement agencies do. As Mr Gray from the Commonwealth DPP has mentioned, part of the issue is the admissibility of the various bits of evidence as you cross the jurisdictional boundaries, because one jurisdiction's admissibility requirements are different from the next. The criminals have no problem with that, but of course we, as law enforcement agencies and policy advisers to government, have to address those sorts of issues. It is important, therefore, for us to learn from the people who are leading the charge—the US is in there as well, and the Europeans are developing a number of initiatives now.

You asked specifically how we keep a tab on that. It would always be nice to be able to have an officer stationed at every OECD and every FATF meeting. We have very close relations with our counterpart officers in the Department of Foreign Affairs and Trade. Where possible, those officers attend and report back to us. We also use the Internet to follow up on all the papers that they produce, and we are getting these official papers within the government system. So we at least feel we are keeping up to date in a policy sense with the initiatives going on in Europe. It could be better, of course, but we do not have officers stationed at each of those meetings. Frankly, we feel we are doing it quite well without that necessity at this stage.

Mr SCHULTZ—Going back to the recruitment side of things, you talk about the possibility of recruiting from the private sector and that you do, in fact, recruit from the AFP. How much recruiting do you do from other law enforcement jurisdictions, like the state police? Given the constant public criticism and, more recently, criticism by the New South Wales Ombudsman about the lack of credibility within the New South Wales Police Service, what sorts of safeguards have you got in terms of checking out people, and what sorts of guarantees in that mechanism can you give that organised crime, through agencies, is not infiltrating the system? It probably sounds a little bit alarmist, but in my time in politics over the years I have been absolutely amazed and very deeply concerned about the way in which organised crime at times has infiltrated our policing agencies. My basic question is: on the issue of recruitment from outside, what sort of intelligence checking do you have that can guarantee that the people that you are recruiting are not influenced by the very capable, well stocked finances of organised crime?

Ms Ellims—Obviously the law enforcement agencies will have to answer this for themselves. But as a preliminary comment, quite often the arrangements involve secondment of existing police officers being shared among jurisdictions, as well as direct recruitment. Just as obviously, there is a security issue—whether it is a secondment or a recruitment process under way—but it is, perhaps, a bit less of an issue if you are seconding an officer who has already been through a process to establish that they are a secure and proper person to employ in the various agencies to whom they fundamentally belong.

Ms Montano—Speaking for AUSTRAC, our IT contractors go through the same protective security clearances as public servants do. We have an additional measure: for example, if someone is brought in to develop a particular thing, they have access only to the development application processes—they do not have access to the entire database of 50 million transactions. We take the view that it is a need to know basis. If to do your job you need X, then that is all you get—you do not get any more. Then we do our normal security clearances in relation to that. They are actually vetted as much as any public servant is. The other issue is, once someone is in, you have then got issues in relation to management of those people. Organisations have audit trails so that if there is an unauthorised access of something it can be traced. So there are a whole range of security measures you have in place to deal with that, whether or not you are talking about a public servant—the private sector does not have the monopoly on people going wrong.

CHAIR—Public servants have occasionally gone off the rails.

Mr SCHULTZ—That is precisely the point that I am raising.

Ms Montano—Yes. The internal security systems, from AUSTRAC's perspective—I can only speak for AUSTRAC in this regard—are the same for public and private sector staff. Money is not the driving factor: that is the point I am trying to make.

Mr SCHULTZ—There are numerous people in our law enforcement agencies that give us an enormous amount of time and expertise because they believe passionately in fighting crime. I am just amazed to hear that we are concentrating to some degree on the issue of not being able to get people into the electronic side of law enforcement—because there is money involved in it. I suppose, to some extent, that was one of the reasons why I asked the first question. If you have got people who are driven by money in terms of working in law enforcement, then why aren't they driven by money in terms of being paid or bought off?

CHAIR—I would not see a strain in compatibility. There are obviously a lot of people who are driven by more than money, but equally I think the reality of life is that a lot of high-tech people will go to jobs where there is more money, but that does not mean to say they are going to be susceptible to accepting money illegally or subject to criminal intentions. They just go and work for Kerry Packer—I have nothing against Kerry Packer, but he can probably pay more than Elizabeth Montano can.

Ms Montano—Can I make a comment about the drivers? It is often far more complex than that, in the sense that, for example, we have IT contractors that come and go; and always when I get the monthly reports on who is coming, who is going and what the recruiting intentions are of our IT manager, I ask the question, 'Why is X going?' And many times it is not an issue of there being more money somewhere else: it is that they are going to work at a bigger facility, or they need new electronic challenges in the sense of new skilling-up. Sometimes for them it is not the money, it is actually their intellectual stimulation.

For some of them, while we continue to do more things and develop new things, that is intellectually stimulating and they will stay with us—even though they might actually be able to get $5 an hour more somewhere else—and many of those people do, by the way, have a Public Service ethos. I have several IT contractors who, whilst they get paid very well, also have a commitment to that sort of work. They would like it both ways, obviously: they would like to get lots of money, but they also like getting lots of money doing work that they think is morally good and socially useful. So we have got a few people who are very motivated that way.

My IT people are not all motivated just by the bucks. We do not pay at the top of the market; we pay, as a policy, in the middle of the market. So we will negotiate people down from what they ask on the basis that AUSTRAC is a nice place to be, as opposed to being somewhere else. Some of their drivers are a bit complicated, but certainly there are also issues of career progression. If you are in an organisation where you are there to do X and you are intellectually capable of more, either technically or in a leadership role, and there is no career path for you, do you stay there? In fact, it may not be in the organisation's interest for you to stay there a long time. Do you get stale? Do you get disillusioned?

It is better for people to have career paths where they can feel that they grow. Money is certainly an issue; but if you actually do talk to a lot of those people who have gone out—and we see a lot of them at conferences: people who have been police officers who then go to the private sector—they still talk about law enforcement at conferences and you can see it is still

their passion, but they have chosen to do it from a private sector point of view where they often see that they are doing the same job, but from another avenue. So money is just one thing.

CHAIR—Can I change direction for a minute? One of the things that has been put to us in some of our evidence and that certainly strikes a note with me is the length of time it seems to take to get legislative amendments in, to respond to the changing world reality out there. I notice Ms Montano is nodding her head vigorously.

The NCA made the point very specifically, and they quoted one example where it took six years to get a legislative amendment through. This committee has certainly experienced some frustrations with the lightning speed with which the government reacted to our last report, the third report, which was in the previous parliament. Even now, we have not actually got the legislation into the parliament yet. Could you tell us: (a), does the department recognise that this is a problem, because it would seem to me that that is tying the hands of the people who need to operate at the sharp end; and (b), if you recognise it is a problem, what are you doing to try to speed the process up a bit?

Ms Ellims—Can I make a general comment before I ask Karl to address the specifics. Elizabeth is nodding but, as she said at the outset of this hearing, in a sense, legislation is a matter of last recourse. You do not leap into legislation until you are quite confident that you are addressing the issue that needs to be addressed, that you are not going to have an unintended effect by so doing and that the evidence is there to convince the parliament that it is proper to enact the particular legislation you are suggesting. There always will be a period for policy development, and of course one wishes, hopes, expects and tries to make it as short as it need be—certainly, no longer than it need be. But it is only proper that there should be a period of policy development to ensure that the legislation the government is suggesting to the parliament is the most effective and proper legislation, that it does, in fact, need to be enacted and that there is not another methodology.

CHAIR—I do not think anybody on this side of the table would disagree with that statement as a statement of principle; nevertheless, given that the crooks of this world are actually able to take advantage of new situations very quickly, it seems to me that sometimes the speed of response from governments is not as quick as one would like.

Ms Ellims—The only other general comment I would make is that legislation has two effects, broadly, in the law enforcement area. It has a very practical effect in facilitating an organisation like the NCA to do its job. It also has a deterrent effect, which is to make it very clear to criminals what the implications are of performing a criminal act. Again, it is extremely important that there be a period of policy development in order not to end up with unintended practical effects arising from legislative change. Some of the legislation that the NCA are particularly keen on seeing tends to be in order to facilitate their processes. In that area it is of course very important that there be policy development that points to the unintended effect—if, indeed, there is going to be one—and makes sure that there is a proper balance between the needs of the community and the needs of the NCA in chasing criminals.

CHAIR—You are anticipating my next question.

Ms Ellims—With those general comments made, I might ask Karl to talk about some of the specifics of your question.

Mr Alderson—In terms of specific measures that policy advisers to government and governments can take to make this whole thing move faster, a key one—instead of a traditional model where the Commonwealth might develop a proposal, have that finalised and then look around at how it compares elsewhere—is actually to have right in that first phase how it will work in our international cooperation, what the models are that they have there and how this will work with the states, and so forth, so that that is part of the very initial advice and cuts out a phase. In this specific area, in terms of having that material and being well placed to move forward next year, it is quite a good situation.

There are two documents, in particular. The cybercrime convention, being developed by the Council of Europe with involvement of a number of other countries, in particular the United States, is a document that draws on expertise and experience from a whole range of countries and is there as a model that all participating countries and others can draw on in terms of offences and enforcement powers. The other one that was mentioned earlier is the Model Criminal Code Officers Committee computer offences report. There was a discussion paper earlier this year, and a report following some more consultation between governments should come out in the near future, perhaps within a few months.

In terms of proactive legislative response that is not always lagging behind, I guess the conceptual leap that is taking place is in trying to think even further ahead. Rather than reacting to current technology, we have to see what kinds of mechanisms can be put in place that do not relate to specific technology. Other than in the law enforcement context, there are models for that in the Electronic Transactions Act. This is an attempt to take that kind of approach, and there have been copyright reforms that try to get away from the idea of specific technology. It may be that we will look back in five years and our attempts to do something that addresses all technology will be seen to be laughable. We have to try to come up with a model that is a bit more lasting instead of addressing a new type of thing every two years. I guess that is another important thing that, as an adviser to the government, we have to focus on so that we are not always following behind.

CHAIR—I hear what you are saying.

Ms Montano—Can I make a comment, because I have been accused of nodding.

CHAIR—No, I must correct the record—not accused; it was an accurate statement, and I have many independent witnesses.

Ms Montano—I may have been nodding about something else. There are two aspects and it is a timing issue. In this area, the really important thing is to think ahead. For instance, if we know that in two to three years time that there is going to be a Council of Europe treaty—and there are going to be EU directives, OECD guidelines and all that about X—and if we think we know what it is going to look like we should be doing the work now. And that is what we are trying to do. So you actually anticipate, so all that legwork is done early. That is what we have been trying to do: pick the future, particularly in relation to things like the FATF's 40

recommendations. They are bound to change. We think we know what some of them are going to be.

We have always been world leaders in that particular forum. We have done reviews before. While everyone else has had to chase around to get their legislation in order, we have already been there. We know the advantages of being ahead. So there are those research and policy development issues before there is a pressing need. And that can certainly cut down time. And there is the issue, as Mr Alderson said, of trying to time proof the legislation so it is not a knee-jerk reaction. It is actually a case of 'let us get back to the basic principles'. Then you get into the big debate of black-letter versus fuzzy, and you have all those sorts of issues. So there is a real minefield of drafting and policy to work through there, but you have got to do that early.

The second issue I make no comment on, except to say that there are parliamentary and government processes where, quite rightly, this area of legislative development has to compete with other areas that governments and parliaments are interested in. There are a whole range of things that obviously you are very interested in looking at, and this lot has to take its place amongst all the rest, and we understand that.

CHAIR—I will call the Attorney-General and tell him to fight a bit harder for his share. I take your point, thank you. It leads on to another general question. I would be interested in the department's attitude to the sorts of criteria to use. I think it is important to get this on the public record. What is the department's view about looking at the balance between effective laws in combating crime and so on, or appropriate powers that you might give to investigatory organisations compared with an individual's civil rights, privacy issues and self-incrimination? I know there are proposals coming up in respect of the NCA where existing self-incrimination laws are being looked at and so on. What approach does the department take there? A lot of people in the community would say, 'Why don't we just do what we have got to do to catch the crooks?' But, clearly, if there is then a situation where—I suppose it is almost part of your unintended consequences—somebody actually gets badly treated by the law, then obviously there is that conflict. Could you talk to us about some of those standards and approaches that you take.

Ms Ellims—I will ask Mr Alderson and Mr Treyde to comment on this. But I agree with you 100 per cent: there has to be a balance between the two. The government would be very concerned about the precedent setting effect—the flow-on, practical effect—if police powers were to be unwarrantedly or improperly draconian. So there always has to be a balance and it is part of the policy process to try to get that balance right. But, that said, the government is very concerned about the range of issues in the criminal world—organised crime in particular—insofar as it relates to drugs, people smuggling and the linkages with money laundering and so on. In fact, the government is putting quite a large resource into looking at the police powers issue, particularly insofar as it relates to the NCA. We hope that work will come to fruition in the not too distant future. Karl, do you want to comment on the policy?

Mr Alderson—There are a couple of points I could add. Firstly, the ideal situation is to find mechanisms that advance law enforcement effectiveness and protection of civil liberties at the same time. Although it does not really come in the new technology domain, you could take, say, the detention and questioning provisions in the Crimes Act, where that one package gave people an explicit set of rights that had been a lot more ambiguous, and it also gave enforcement

agencies a clear set of powers. Various commentators have seen that package as a positive from both perspectives.

Secondly, it ties in with the earlier question you raised about hastening the process. One thing that can assist with that is for those kinds of considerations—the need to protect privacy and prevent abuse of powers and so forth—to be factored in right at the start rather than there being a focus on one side or the other and then there being a protracted debate that can bog down the process. In terms of the process that is gone through, I guess one of the fundamental roles of the department is to seek to draw those threads together and there is a specific unit that deals with privacy issues. More generally, everyone has a responsibility to look at the proposals and see that they do not involve risk of abuse of powers, and then to ask what the other accountability measures are that form part of it and so forth. I guess getting those things early helps to minimise delays in the legislative process.

Mr Treyde—I would like to make a few additional comments very specifically in relation to TI. That act allows for the interception of communications. It is basically an investigative tool that is regarded as being highly intrusive, so it is an area where privacy issues are particularly important. That legislation establishes a regime which attempts to guard the privacy of individuals in that the interception of communications is allowed only in certain limited circumstances, and then the handling of the information that is gleaned from those interceptions is carefully controlled. Ultimately, the records and so on are destroyed, and there is the monitoring of the agencies themselves that gather that information. So there is a recognition of the need to protect privacy and, where possible, the policy is to enshrine some sort of protective mechanism. That actually comes back to the question that was asked much earlier about the sharing of information with foreign bodies. The protection of privacy is an important consideration. If the department were to look at ways in which such information might be shared with foreign agencies, there is always the underlying issue of how you can ensure that you can protect the privacy of Australian individuals when this information is passed to foreign organisations.

CHAIR—Earlier this morning, somebody said—and I think it might have been Ms Montano, but I could be slandering you—something to the effect that ASIC, AFP and NCA deal with the same types of crimes, and therefore my question to the department is: why not the same powers? They have all got slightly different powers, have they not, and yet if they are dealing fundamentally with the same crimes why not the same powers? And you could almost wrap ASIO into that context.

Ms Ellims—One part of the answer is that they have different roles and different focuses and that is why there are different bodies. Successive governments—because all of these bodies were not established by the current government—have taken the view that there needed to be a discrete and significant resource in each of those cases devoted to the particular focus that they bring to bear on the range of crimes, some of which will be the same crimes.

Ms Montano—It was me but I do not think I said ‘same crimes’. I said that there might be different crimes but the criminals often used the same infrastructure, or they leveraged off it.

CHAIR—I was not trying to mislead—

Ms Montano—That is all right. There are parallels and, while it is obviously not necessarily the answer for everyone to have the same thing, they should be complementary. If you are talking about, in an overall infrastructure of criminal law, what sorts of regulatory measures you put in place to help law enforcement rather than hinder it and what sorts of powers and tools you give them, they may not be exactly the same for each agency but they should be complementary. There should be policy reasons that are sensible and thought out for why there are differences and similarities, rather than things developing in a different way, which is why our AGEC is cross portfolio. We actually have been trying to do that—thinking about what the common interests are.

I will give you an example. The Internet Industry Association is having discussions with law enforcement agencies. It is not in anyone's interests, either the public sector or the private sector, for the agencies which need to talk to the ISPs to make totally different approaches. I encourage them, all being members of the AGEC, to go with a united view as far as they can. Their views may not be identical but at least they can be consistent; otherwise you get a situation where the ISPs say, 'Hold on a minute. Agency X said that they wanted us to do Y last week and now you are saying you want something else. Why can't you people talk to each other first?' There will be differences and they do want different logs for different purposes—revenue is different again because what they like to have is different in some ways to what law enforcement agencies need, for good reasons—but as far as possible they should be consistent. That is what we have been trying to do—to get them to consistently develop principles. Then when an individual agency has to go beyond and say, 'But for our special purposes we need X as well,' at least it all fits in. It is not necessary that they all need to do the same but they certainly should be consistent, which is why you hope that things are actually looked at holistically.

Ms Ellims—I have just one more comment in relation to that question and that is that because these agencies have a different focus and a different role—they are set up to perform certain things and not other things—the question of sharing their powers becomes quite a deep policy question that needs to be considered from time to time. One of the quite interesting developments in the last two to three years has been a greater propensity to share information at a holistic level between law enforcement and security agencies, by which I mean that security agencies may be aware of certain new technology which may also be of use to law enforcement but law enforcement may not be quite in the same position to become aware of it. At that level, in the last two to three years, there has been a greater sharing of information, which is obviously to the good and to the benefit of law enforcement, and sometimes also to the benefit of security agencies. But when it comes to the question of sharing of powers, there is quite a significant policy question to be addressed, which is whether or not powers that, for example, security agencies might have are appropriate to be exercised by law enforcement agencies.

CHAIR—Marshall Irwin from the NCA spoke to us approvingly about the UK's Regulation of Investigatory Powers Act 2000, which I am sure you are familiar with. Given that we have got a federal system obviously that is a bit of a problem, although Britain is fragmenting in some senses, of course. I do not say that unkindly—it is just a statement of fact. Would you see that act as a good model for us if it could be adapted to our context?

Mr Alderson—I can say that it has been a very closely examined model, in terms of the work of the Model Criminal Code Officers Committee. Traditionally, Australia has always turned to

certain countries, and Britain is obviously one of the key countries, and that piece of legislation is receiving very close attention in the development of those recommendations.

CHAIR—Okay. The last question—and I think this is probably for AUSTRAC, Customs, the DPP and maybe even CrimTrac—is whether or not you have concerns about the budgetary impacts for your respective organisations from the development of new technology. What type of impact is involved in terms of getting new equipment—that sort of thing? This stuff often does not come cheaply. I have just upgraded my PC at home, having bought it 15 months ago or something, and I had an expert come along and tell me, 'You have not got enough of this and you have not got enough of that and all the software is out of date,' so I have just spent a fortune upgrading that. I would be interested in your comments about the budgetary impacts of the changes in technology and whether you have got particular priorities that you would want the committee to give attention to in the context of this inquiry, especially perhaps of a law reform nature.

Ms Ellims—As a general comment, I believe the agencies do have concerns about the potential budgetary impact of keeping up with new technology. There has been a range of budget measures, which you have probably seen in looking through the budget papers over the last few years, where the government has committed quite significant resources to the agencies in the area of new technology, in part in the area of development—understanding the kind of new technology that is wanted. The cost, of course, is greatest for the purchase of the capital infrastructure. CrimTrac is one of the most notable, and in some of the other agencies—Customs and the AFP, for example—there has been some money devoted to developmental purposes. I think it goes without saying that there is a concern about the potential impact of cost for new technology for all of the agencies. One of the strategies which the agencies are employing now, and will need to employ more in the future, is the sharing or partnership strategy—the integrated approach to new technology. Certainly they and we are very keen to do that and that sort of work is progressing quite well at this stage. I will hand over to the agencies to comment more specifically.

CHAIR—Customs, do you have anything to say? Do you want more money?

Mr Naylor—Have you known a public servant to say no? Whilst we have certainly had significant input of funding in relation to new technology which would not necessarily be specifically associated with e-commerce—I am talking in terms of X-ray machines and the like: there has been enormous investment by Customs, or by government through Customs, in that range of technology—with regard to the budgetary impact of the developments in terms of IT and electronic commerce, certainly I support Sandra's view that, yes, we are concerned. We have not at the moment got major sources of funds to invest in that sort of thing but I certainly support Sandra's view that the agencies of the portfolio—and I think outside the portfolio in state governments as well—are looking to work much closer together and to have a unified and integrated approach to this sort of thing.

In terms of the likely availability of hard cash in due course, I think it is very much an unknown quantity at this stage. But the sophistication which is available to the bad guys is an implication that it has to be available to the guys in white hats as well in due course.

CHAIR—Does the AFP want to add anything?

Mrs Grant—Could I just add a little bit on behalf of Customs. Customs is actually investing quite a lot of its own funding at this point in time in our cargo management re-engineering process, which is a process where we are looking at business process redesign, as well as completely overhauling our commercial computer applications which we interface with the importing and exporting community. That is a significant investment from within. With a lot of the issues that we have been talking about this morning we have to build the safeguards into those systems to keep the security of the information. We are also going to be building in some artificial intelligence aspects in the system so that we can identify high risk transactions. It is, of course, a concern to us that Customs be on the front foot in trying to keep ahead of the game.

Mr Walters—The issue of the budget is something that the AFP would like to address to the committee when we appear early in the new year.

Ms Montano—Money for things is always an issue but more than that I think we are seeing now is that part of that cooperative, holistic approach is about what I call 'thinking' money. There are two categories of money in this sort of area: 'thinking' money—what should we be doing—and then there is actually the 'doing' money. Historically, agencies have always focused on the doing money. The thinking money is, in fact, difficult. To give an example—I am not crying poor because it is something that government has directed us to do and I have been very pleased to do it because I think it is very important that it be done—while AUSTRAC has had a big role in relation to some of this research work, we have not got any extra money to do that. That is being done on an ad hoc basis along with everything else. Often this work does not move as fast as it could, because obviously my first priority is AUSTRAC core work and the other agencies could say the same thing about their R&D issues. The smaller you are as an agency, the less there is to actually put aside to that sort of thing. Thinking time is a bit of a luxury sometimes. If someone could give me more time to actually sit down and think about these issues in the longer term that would be good.

CHAIR—I think that could apply to many of us.

Ms Montano—Yes, exactly. It is an issue of the thinking and the issue of 'what should we be doing now' that in three or four years time we will say was smart time spent, as opposed to just reacting to what is happening now. I think there are three issues. There is that issue of thinking, research and development. Research and development is a term which can mean lots of things and often it does not have a lot of discipline attached to it. But if, in fact, it is disciplined then that can be very useful.

The second issue is the legislation issue. Yes, certainly, once you have done the thinking you actually want something to happen pretty quickly so that the thinking actually has effect—but we have had that discussion. The third issue is: how do you actually put into practice what it is you have thought of that has been very smart in the last year or so? It is never just a matter of throwing money at it; it is far more complicated actually.

Mr Gray—I had not thought of it in terms of research funding until two minutes ago but it sounds like a good idea and something I would support. Because the DPP is an end-user of the evidence the investment, I think, has to come in in the upstream, investigative agencies. So as far as I am aware we have not got a funding issue in relation to developing in-house systems. I suppose the thing we have developed that is worth mentioning—the sort of plus side of all this

electronic commerce and electronic development—is the litigation support system which is presenting cases electronically. It is worth mentioning that because we tend to look constantly, I suppose, at the negative and the insurmountable challenges of some of this stuff. There are positives from law enforcement and the ability to run these big cases. It is mainly used in the corporations area and you just cannot run those cases without the sort of technology which is available. Apart from research funding, I would support everything that Ms Montano has said.

CHAIR—Does CrimTrac have anything to add?

Mr Terrell—Resources are always an issue driving the CrimTrac agency in terms of what we are trying to deliver. The agency is a bit different in that it is not purely Commonwealth; it is established as an executive agency under the Public Service Act. So in one sense it is an entirely independent Commonwealth agency, but it also operates under an intergovernmental agreement signed by all police ministers. Our charter is very simply to deliver advanced information services and investigation tools to the nation's police. So a lot of what we are doing is very much driven by the fact that the clients, the police services, are responsible for the long-term funding of CrimTrac. The federal government has committed $50 million to build our four major new national systems: the national DNA system, a new fingerprint system, a child sex offender system, and much better access to information across jurisdictions, across state and territory borders.

We are well funded from that point of view, but we are very conscious of the fact that we cannot put in a system which is going to cost the police services an arm and a leg to run once the capital injection is used. We are also very conscious of the future in terms of other national systems that might be on the horizon. I would like to echo that there is, I think, a lot of positive feeling about what the police nationally want to get out of IT and how they approach what has always been a very difficult issue in terms of information sharing and exchange.

The new things, like the DNA system and the replacement fingerprint system, in themselves will produce many benefits to Australian policing. The agency as a service provider is there not only to implement the systems but also to assist the jurisdictions in taking them up. But there are always going to be resources issues; there are always going to be new systems which the police will want; there will always be priorities within government as to where the money goes both at the federal and state levels. It is always going to be a matter of making sure that your case is a good case.

CHAIR—Thank you very much.

Mr Alderson—May I correct an earlier answer? The regulated investigatory procedures act is being closely considered by this department in terms of reviewing enforcement powers. I said the Model Criminal Code Officers Committee are looking at the English computer offences legislation, which is a different act.

CHAIR—Thank you very much. Let me say that I have in the past been known to be critical of A-G's when I thought they had not given us an adequate submission. I want to put on the record that I think it has been a very worthwhile submission and obviously a lot of work has gone into it. We thank you for coming here today. I think the hearing has been very interesting.

We may have further questions further down the track, in which case we will obviously be in touch. Thank you to everybody for coming.

Committee adjourned at 12.07 p.m.