COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE ON THE AUSTRALIAN CRIME COMMISSION

Reference: Cybercrime

MONDAY, 21 JULY 2003

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 AUSTRALIAN CRIME COMMISSION

Monday, 21 July 2003

Members: Mr Baird (Chair), Mr Sercombe (Deputy Chair), Senators Denman, Ferris, Greig, Hutchins and McGauran and Mr Dutton, Mr Kerr and Mr Cameron Thompson

Senators and members in attendance: Senators Greig and Hutchins and Mr Baird and Mr Sercombe

Terms of reference for the inquiry:

To inquire into and report on:

Recent trends in practices and methods of cybercrime with particular reference to:

1. child pornography and associated paedophile activity;
2. banking, including credit card fraud and money laundering; and
3. threats to national critical infrastructure

WITNESSES

Committee met at 9.09 a.m.

GRABOSKY, Professor Peter Nils (Private capacity)

CHAIR—I declare open this public meeting of the parliamentary Joint Committee on the Australian Crime Commission. The committee is examining recent trends in practices and methods of cybercrime, with particular reference to child pornography and associated paedophile activity; banking, including credit card fraud and money laundering; and threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly-established Australian Crime Commission might play in combating this crime.

I welcome our first witness, Professor Grabosky. As you are aware, we prefer evidence to be given in public, but if at some stage you wish to go in camera please put your request through to the committee and we will consider it. I now invite you to make an opening statement.

Prof. Grabosky—First of all, I thank the committee for inviting me here this morning. Some weeks ago I sent to the committee copies of a few articles I have written or co-authored on the subject of cybercrime. They included articles on online child pornography, online fraud and cyberterrorism. All of these were based on open-source information, and all have been published. I hope that the committee has found some of them to be useful.

I believe that our work has generally stood the test of time, with two exceptions. At the time that my colleagues and I wrote the article on child pornography in the digital age, some five years ago, we were unaware of any commercial transactions involving such material. Since that time, I have seen reports of child pornography cases involving online commercial transactions. Our book entitled *Electronic Theft* was completed in 2000 and published in 2001. It deals with online fraud, extortion, piracy, share market manipulation and other crimes of acquisition but makes only passing reference to fraud relating to online auctions. This has since become a significant problem. I have a few short observations, and then I would be happy to answer to the best of my ability any questions you might have.

Many victims of cybercrime are reluctant to report their victimisation to the police. In the case of institutional victims, this reluctance arises largely from commercial considerations: the desire to avoid adverse publicity. Obviously, the victim's interests here conflict with the interests of law enforcement to have as full a picture as possible of cybercrime. There is no perfect solution to this problem. Two solutions, each imperfect, might merit consideration by law reform bodies: first, confidentiality agreements between law enforcement and the victim in cases that do not lead to prosecution; second, statutory prohibitions on disclosure of the victim's identity, or suppression orders, in cases that are prosecuted.

The growth and pervasiveness of digital technology mean that the day is approaching when nearly every ordinary crime scene will have some digital evidence. The growth and pervasiveness of digital technology also mean that the volume of cybercrime will continue to outpace the capacities of law enforcement agencies to deal with it. This means that law enforcement agencies will be well advised to choose their priorities carefully and that the control of cybercrime will require prospective victims to exercise greater responsibility for their own cybersecurity.

The cross-border nature of cybercrime—both within the federal system and globally—means that coordination between law enforcement agencies will be very important. Lack of coordination will mean that scarce resources and different jurisdictions will be at risk of reinventing the wheel or duplicating their activities, or of allowing matters to fall between the cracks, so to speak. Given that most critical infrastructure resides in private sector hands and that private sector interests command a great deal of expertise in matters of cybersecurity, coordination between law enforcement agencies and the private sector will also be very important. Law enforcement agencies and governments generally may wish to avoid activities and services that can be as effectively delivered by the private sector.

One additional issue that might merit discussion is the legality of what might be called 'remote cross-border searches'. In other words, assuming I am under investigation for a crime in Australia, what legal authority is required by an Australian law enforcement agency to search for evidence of that crime which may be stored on a server in China but accessible remotely from my computer at the ANU? Would a search without the knowledge of Chinese authorities invite reciprocity?

Thank you for your patience. If you have any questions, I will do my best to answer them.

CHAIR—Thanks very much, Professor Grabosky. My first question relates to the issue of child pornography. In your paper you point out the difficulties of trying to control child pornography on the Internet. Was it five years ago that you wrote the paper?

Prof. Grabosky—Yes.

CHAIR—I wonder whether you have changed your views since you wrote the article five years ago. Do you think the most effective measure is parental control in the area?

Prof. Grabosky—The first line of defence is parental control, for sure. The medium of the Internet, as you know, is one that makes control very difficult. With specific reference to child pornography, you would be aware that a good deal of that material is exchanged in private between individuals rather than being broadcast. The interdiction of private communications on the Internet is a daunting task.

CHAIR—Given your experience in the area, do you have any recommendations? While it is a daunting task, what do you believe are effective steps that we could take in gaining some form of control?

Prof. Grabosky—I think the kinds of investigations that have proven successful merit some consideration—for example, cases involving the prosecution of individuals who may have attracted the attention of law enforcement for other, perhaps unrelated reasons. In the course of investigations, some evidence of illicit materials has been found on their computer, perhaps leading to a trail of other offenders with whom that individual may have been in contact.

CHAIR—That certainly has some merit. When someone is brought into custody on a child sex offence matter, I would think it unlikely that there would be any checking of their Internet to see to what extent they have been downloading child pornographic material and to use it to follow through in terms of other individuals with whom they have had contact. I think that is an

interesting proposal. In terms of a community education program, do you think that is worth while? What form should it take? How extensive should it be?

Prof. Grabosky—Let me backtrack for a second. Obviously I would want to exercise some caution in the conduct of investigations lest innocent persons on the mailing list of the target of investigation be implicated.

With regard to public information campaigns, there have been examples of what might be described as parental guidance messages, safe-use messages: 'Be mindful of what your children are doing online' and so on. It is a difficult question the older a child becomes, in terms of ensuring their privacy as well. The fundamentals of good parenting are important. I do not have a quick solution as to how most efficiently and effectively to impart those basic principles. One wonders about the extent to which that is a law enforcement function as opposed to something that could be done by other agencies, public, private or non-profit. I am mindful of the fact that law enforcement resources, both in terms of their forensic computing capacity as well as their conventional terrestrial policing capacities, are constrained in most places in the world. One wants to marshal those resources in a manner that will lead them to deliver the most efficient and effective outcomes.

Senator HUTCHINS—You talked about reluctance to report, particularly in terms of child pornography. I wonder if you could comment on this. We have a submission on the privacy aspects of the relationship between sending and receiving. If I received an email which contained child pornography and I opened it, would I be committing an offence there? Would that reluctance be for me to report that to the police because I have opened it? I wonder if you would like to comment on that particular aspect.

Prof. Grabosky—That is a difficult question. My commitment to principles of truth in labelling compel me to disclose here that I am not a lawyer. My formal qualifications are in political science. I would be reticent in giving you an authoritative judgment on where criminal liability sets in in the scenario that you have just described. I have had a glance at the submission that Electronic Frontiers Australia have made to this committee. From what I recall, their assessment is that the law of possession varies somewhat across the federation and it is not inconceivable that someone could incur criminal liability through unintentional acquisition of those materials. In my prefatory remarks, my reference to the reluctance to report referred primarily to institutional victims of financial crime: financial institutions that have been defrauded. Their primary inhibition was the concern to avoid adverse publicity. Obviously one could envisage a reluctance to report here that relates to that.

Senator HUTCHINS—I cannot go into a bookshop in Sydney and buy child pornography, because it is banned. Is there technology that stops it being broadcast to me?

Prof. Grabosky—This is a complex question because of the nature of the Internet, which transcends national boundaries. I could, hypothetically, acquire materials from an individual on the other side of the world in the course of a private exchange of communication. It would be extremely difficult to interdict those communications, especially since they could be concealed through the technologies of encryption, steganography and so on, which would make it very difficult for anyone to determine the content of that communication.

Senator HUTCHINS—We will move on from child pornography to, say, business institutions—is there technology that can protect them from having a virus put into their system? I sent my second email the other day, in all the years I have had a computer, so I am a Neanderthal in that way. I am pretty sure my colleagues might be a bit more advanced.

Mr SERCOMBE—You are too modest.

Prof. Grabosky—One may wish to distinguish between the willing acquisition of illicit material—that is, the exchange of child pornography between afficionados of that material—and the unwitting receipt by an individual of illicit material. We all get spam junk mail every day—certainly I do; I get at least two advertisements for Viagra every day.

Senator HUTCHINS—You should not have replied to the first one!

Prof. Grabosky—It all goes into the trash, I'm afraid. Screening and blocking unwanted incoming communications is conceivable, and there are technologies that can assist there. Similarly, security technologies that are used in large financial institutions are really quite sophisticated.

Senator HUTCHINS—Is there anything that technology can do to outsmart people who are trying to push pornography or trying to put bugs into systems? Can a proactive position be put, rather than being reactive?

Prof. Grabosky—Indeed. The development of what are generically referred to as blocking and filtering technologies can help screen communications so that unwanted communications are automatically rebuffed, discarded or deleted. The problem there is how fine the mesh is and whether certain communications which one would want to receive might be excluded by a mesh that is too fine.

Senator HUTCHINS—Do you think people are generally aware of the risks that they run in terms of using the Internet for banking and for purchasing shares et cetera? Do you think the risks outweigh the benefits or vice versa? Do you think people are aware of the risks?

Prof. Grabosky—I would imagine that you have those people who are quite naïve about risks. These are the kinds of people who, for example, keep their PIN number right next to their debit card or post their password on the computer screen with a yellow sticky label. But there are others who are more sophisticated and who do take appropriate precautions. I would imagine that sensitivity to these security concerns is developing all the time. Technological solutions or partial solutions are important and are being developed and deployed, but I think the ease and convenience of electronic transactions are such that that is where the future is. I think most people would regard the convenience of electronic transactions as offsetting whatever risks they might face. To be sure, there are people who still want to keep their money under the mattress, so to speak; but by and large I think the digital age is upon us, and most knowledgeable people, and certainly knowledgeable institutions, engage in appropriate risk management practices.

CHAIR—We welcome Senator Greig to the committee.

Mr SERCOMBE—Mr Chairman, I would be interested in talking to the professor further on this issue of material that exploits children. As I see it, and based upon some of the evidence we have already had, there is obviously a range of very complex issues. This matter of parental supervision, for example, is all very well, but with kids having 3G technology in terms of Internet access now there is a notion that children will always have parental supervision at home, which is clearly not correct.

Another issue is, I suppose, the whole definition of what people regard as pornography. I think there would be a pretty broad community consensus about what hard-core child pornography is in our current environment. However, I am very conscious of the fact that over time and in different cultures that perception changes and moves, and what was pornography in Victorian England is not necessarily pornography now. So there are issues about definition.

A further issue is where the priorities of law enforcement ought to be in this. If we raise undue expectations in the community about what law enforcement can do, they are inevitably going to be disappointed. I would welcome your comments on where priorities really ought to go, given that law enforcement resources are limited, even if they are beefed up. For example, the Victoria Police said to us the other day, in response to some questions I was asking, that the more sophisticated exploiter of a child—the more predatory type of individual—is fairly unlikely to get picked up with the sorts of checks that are presently conducted, simply because they, at one level, may use encryption to transmit material between themselves and their peers.

The issue really at the heart of a lot of community concern, particularly about children being groomed on the Internet, is that catastrophic circumstances can arise if a child meets a predator. I particularly asked the Victorian police about the notorious set of murders in Victoria involving a fellow called Mr Cruel, who the police still, I think, have not caught. I said: 'Did you have any chance of catching Mr Cruel by random surveillance of the Net?' The senior sergeant who I was speaking to was closely involved in that investigation and clearly said, 'There is no way, from what we know of this character, that we would catch him in that sort of dragnet.'

It seems to me that, in terms of community priorities, the crucial thing is giving the community some assurance that the worst-case scenarios are minimised, rather than trying to hold the tide back, if you like, by concentrating on the peripheral. I am sorry about that long, meandering set of statements rather than questions, but I would be very grateful for your views on where, in a limited-resource environment, you could put priorities to address some of the underlying problems, which really are about protecting children.

Prof. Grabosky—Given the fact that resources are limited, and given the fact that parliaments have seen fit to proscribe a vast range of activities of varying degrees of heinousness, this is a fundamental concern. Ultimately it is a political judgment as to how the limited resources available to law enforcement will be deployed. I would be guided by the insights of some of the law enforcement spokespeople that will follow me in terms of what they would regard as the most productive allocation of their resources.

It seems to me that deploying a significant number of law enforcement officers to visit teenage chat rooms in the hope that they may encounter one offender is not necessarily a recipe for success. One would want to be mindful of the efficiency, as well as the effectiveness, of that particular crime control strategy. There may well be other approaches that would yield more

productive outcomes—rather than the random monitoring of chat rooms, perhaps the strategic targeting of particular suspects.

Mr SERCOMBE—If the purpose of the exercise at the end of the day is essentially about protecting children—and I think that is clearly what it is about—what can criminologists tell us about the profile of the predators, as distinct from the sort of person who might have a particularly warped sexual view of the world or who simply sits in a chat room and talks to kids? I would have thought that the real interest in the community would be focusing on the person who is a serious threat to the security and the safety of children and that they are the areas in which criminology can potentially help us in identifying the profile. It would be nice to have a policeman on every street corner and it would be nice to have a policeman in every chat room, but the realities are that that is not going to happen. How can criminology assist in identifying the profile of the sorts of people we really ought to be worried about, or is the continuum just too hard to make a prediction about the point at which a person is a serious threat to children?

Prof. Grabosky—It is very difficult to do that.

Mr SERCOMBE—I am sure it is.

Prof. Grabosky—I would say that the best predictor of offending against children is previous offending against children. Once a predisposition becomes apparent, it is a risk that is likely to be fairly enduring. We do know that this is a fairly robust behavioural predisposition. So, if you were to present me with 20 people and ask me to pick the person most likely to offend in future, I would say that, if any of them has a previous conviction, that would be my best clue as to the likely offender.

CHAIR—Given that, what would you do in terms of the area that we are looking at—the Internet? If somebody has had a conviction—and you say that these people are the most likely to reoffend—should there be some controls on their access to the Internet?

Mr SERCOMBE—For example, a convicted sex offender will have a limitation placed on their capacity to go near a school. Is it feasible to contemplate a situation where offenders with sexual convictions have sanctions in relation to access to IT if in fact a causal link is demonstrated?

Prof. Grabosky—We have moved from more general prevention to specific post-conviction remedies.

Mr SERCOMBE—I say that because you say that the best predictor is a previous offence.

Prof. Grabosky—There are a number of conditions one can impose on a convicted offender as a condition of liberty—probation, parole, whatever—that can entail restrictions on that person's use of Internet technology. Obviously, to require that a person avoid all contact with digital technology, full stop, is impossible in this digital age. However, there are certain conditions that one could impose on a convicted sex offender regarding their use of Internet technology, for example. One could require the installation of monitoring devices as a condition of probation or parole that would allow authorities to monitor that individual's compliance with

the condition imposed upon him. These are fairly intrusive, of course, but we are talking about convicted offenders.

Mr SERCOMBE—What can criminologists tell us about the progression of the sort of person who may be in an Internet chat room chatting up kids? I hear what you say about the best predictor of a serious offender being someone who has already offended, but, whilst it is offensive to the community to have someone sitting in a chat room chatting up a kid, in terms of the grade of threat to the community and the child's safety I would have thought that it would be at the relatively lower end. It becomes a serious problem if there is a seeking of some sort of physical contact, for example, or if there is the actual commission of an offence. But what can you tell us about the propensity of someone who is predisposed to sit in a chat room talking to kids to ultimately go through the spectrum of offensive behaviour, in the community's eyes, to something significantly worse? Is it something which occurs irregularly or is it a common progression? What can you tell us about the profile of the sort of people we are talking about?

Prof. Grabosky—I am not an aficionado of chat rooms of any kind, personally, but obviously there are individuals who will visit chat rooms and engage in fantasy behaviour but never act on fantasies.

Mr SERCOMBE—Is that the more common profile?

Prof. Grabosky—I could not give you a quantitative assessment of that. There are obviously people who prey upon children without making any kind of electronic contact with them; it could be outside schoolyards, at bus stops, playgrounds et cetera. Then there are individuals who make electronic introductions and then follow those up in the real world, as it were. I could not give you a profile as to the proportion of child sex offenders who operate in each of those—

Mr SERCOMBE—Do you know whether research been carried out in Australia on that matter?

Prof. Grabosky—I am not familiar with it. That is not to say that it has not been—

Mr SERCOMBE—Would the Institute of Criminology be able to point us in the direction of anything on that? What is important, in my mind, is to get a sense of the order of the problem and the prognosis. If the overwhelming evidence is that the fairly bizarre behaviour—from a community point of view—of sitting in a chat room and chatting to kids is unlikely, based on experience, to go on to serious offences against kids, the question of resource allocation to it takes a lower priority. If, however, the evidence is to the contrary, it seems a powerful argument for putting considerable resources into it. But to make that sort of judgment it has got to be backed up by research, I would have thought.

Prof. Grabosky—I could not speak with authority about whether the Institute of Criminology could address that question. I have not worked there for a couple of years now. It is a research question that is extremely difficult to address, because some of the behaviour, as we have suggested, may well occur below the surface, as it were. We were speaking about people who engage in fantasy behaviour, never disclose their true identity and never proceed any further. This is behaviour that even the innocent participant might not be aware of. Quantifying that is extremely difficult. I am sorry that I cannot be more positive in response. From what I

understand, lots of people indulge in fantasies on the Internet. Some of them are not very healthy fantasies—some of them are quite grotesque and horrific—but they are not acted on.

Senator GREIG—I think we understand the difficulties of trying to capture somebody who might be engaging in this behaviour. Mr Sercombe raised the point about the rapid evolution of the technology and it being less geographically situated in terms of G3 and emerging technologies, but I was thinking more about authorities trying to home in and catch somebody who is engaging in this behaviour. Do you have to catch the person at the time they are engaging in this behaviour or can you simply locate the computer?

Prof. Grabosky—Are you referring to the use of chat rooms to arrange meetings with children?

Senator GREIG—Yes, indeed. It would be possible for somebody simply to move around Internet cafes and not necessarily engage in their behaviour from home, in which case the geographical location of the offender would be very difficult to pinpoint.

Prof. Grabosky—That would of course pose challenges, although presumably the email facility that one would access through the Internet cafe might permit identification of the perpetrator. Some of the most sophisticated electronic crimes are committed by people who loop and weave their communications through servers in different jurisdictions around the world. This makes it very difficult to find out where they are from. I know of one such case in Hong Kong. It was a stalking case. The victim complained to the authorities and they tracked the offending communication to a server in Colorado. The investigators from Hong Kong flew to Colorado and discovered when they got to Colorado that the communication had originated in Hong Kong. But that is the nature of cyberspace. Communications can be routed in a convoluted fashion all over, making detection very difficult.

Senator GREIG—Do we have enough international cooperation in coordinating necessary legislative responses to these emerging technologies? I should imagine that many jurisdictions have different, possibly even conflicting ways in which they approach cybercrime.

Prof. Grabosky—There are certain types of activities where a meeting of the minds, as it were, or harmonisation would seem least likely—for example, some types of content regulations. Neo-Nazi propaganda, for example, is criminal in Germany but is protected speech in the United States. I would say that harmonisation at that level, and with that particular type of communication, is in the too-hard basket, but the developed nations in the world have made very significant progress in harmonising law and policy with regard to many other types of offences. Probably the greatest prospect of harmonisation is in the area of child sex offences, where most nations of the world—certainly in the developed world—regard this as very serious, unacceptable behaviour and have mobilised significant resources to attempt to control it. Through groups such as the G8, the Council of Europe and APEC, there are attempts to harmonise law and policy and to establish networks. Mr MacGibbon will be able to describe some of those international network arrangements in much greater detail.

Significant progress has been made in harmonising laws and in coordinating investigative capabilities. You will have seen over the past few years some very sophisticated investigations that resulted in simultaneous raids by authorities in a number of countries, which I think is

testimony to the capacity of law enforcement, at least in the developed world, to really cooperate effectively. Where the problems arise is in the less developed world, where nations just do not have the legal capacity or the resources to keep track of electronic illegality in the way that nations such as Australia, the United States and the United Kingdom have been able to.

Senator GREIG—In your submission, some of what you are saying comes back to the issue of parental guidance and education. Do you think that is an area where we as a parliament could do more? I know we have the NetAlert organisation, which has been up and running for a few years and which was recently re-funded for a further two years. Do you think that is an organisation that is best placed to begin that kind of advocacy in terms of educating parents, communities and schools about the way in which we should approach the Internet?

Prof. Grabosky—I am not familiar with the particular organisation you referred to. Because schools are so pervasive in Australian society, they are able to reach parents and children as effectively as any other institution, if not more so. If you look at the basic institutions in Australian society where there is some contact with current or prospective parents—schools, religious institutions and so on—there are channels of communication that could be used for communication of appropriate precautionary materials. Having said that, you cannot press a switch and have everybody reach a state of enlightenment. Look at health promotion messages: we spend a lot of money promoting health, but there are people who for one reason or another persist in disregarding that wise counsel and continue in their own risky lifestyles. Our best efforts to improve the quality of parenting in Australia will not be universally successful. That is not to say that we should not keep trying to improve the quality of parenting, but I do not think there is a magic bullet.

CHAIR—It would appear that ciphering equipment, such as Net Nanny and so on, is not fully effective, especially with chat rooms, where clearly we have demonstrated how easy it is for someone to go straight in and filter that out. Do you have any suggestions about what we might recommend in that regard? If the technology is not fully effective, perhaps it is creating a false sense of security in parents such that they may not monitor as much as necessary, particular with regard to chat rooms.

Prof. Grabosky—There is a distinction between interdicting communication between two willing participants and an individual accessing materials that are available more broadly on the Internet. Blocking and filtering software are more effective in the latter—that is, if I had a child, and I wanted that child not to access sexually explicit material, I could program the computer to do its best to block his access to various explicit web sites et cetera. I could also, presumably, program it to prevent him from accessing chat rooms as well, or I could seek to program it to prevent his accessing certain chat rooms and not others. I could also obtain some indication as to what chat rooms he visited and when during a particular period of time, but it is very difficult to regulate the content of the child's communication whilst in the chat room.

CHAIR—I understand that it is still possible to infiltrate even the most benign chat rooms.

Prof. Grabosky—There are some chat rooms that are limited to individual subscribers on a private basis, and there are others that are open to the world.

CHAIR—There being no further questions, thanks very much for coming today, Professor Grabosky. We appreciate your time and your input.

[10.05 a.m.]

KLEIN, Mr Nicholas Elliot, Team Leader, Intelligence Development, Australian High Tech Crime Centre

MacGIBBON, Federal Agent Alastair, Director, Australian High Tech Crime Centre

CHAIR—I welcome representatives from the Australian High Tech Crime Centre. The committee is examining recent trends in practices and methods of cybercrime, with particular reference to child pornography and associated paedophile activity; banking, including credit card fraud and money laundering; and threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime. As you are aware, we prefer all evidence to be given in public, but if at some stage you wish to go in camera please advise the committee and we will consider your request. I now invite you to make some opening comments.

Federal Agent MacGibbon—The Australian High Tech Crime Centre welcomes the opportunity to appear before the parliamentary Joint Statutory Committee on the Australian Crime Commission. We particularly welcome efforts on the part of the joint committee to demystify some of the key aspects of cybercrime, or—as we prefer to call it—high-tech crime. The Australian High Tech Crime Centre is a new capability for Australian law enforcement. It was formed as a result of agreements between Australian state, territory and Commonwealth governments and police services to address high-tech crimes in a nationally consistent and coordinated fashion.

The first stage of the centre was launched on 2 July 2003, less than three weeks ago. I say 'first stage' because we recognise that the centre will undergo a series of evolutionary changes before we will have the capabilities, processes, systems and strategic agreements in place to make a consistent and significant impact on high-tech crimes affecting Australians. We do not fool ourselves into thinking that these changes will be easy.

The centre operates in an enormous spectrum, defined by a diverse range of crime types overlayed across all Australian jurisdictions and overseas, within a technological environment which has exhibited exponential growth. All of this has occurred in an environment over the last decade in which the dominant thinking was that an untamed and unregulated Internet was inevitable.

We contend that, while activities on the Internet are 'virtual', they still rely upon the physical world. Wherever the Internet and those who use it rely upon the physical world, we can influence it. Online criminals actually have a physical presence, and law enforcement agencies need to find that presence and move against those people, just as they do against other criminals. Equally, we recognise that victims of crimes committed 'virtually' are real victims and that the crimes committed against them are also real. Of course, the Internet will never be free of crime, but it is fair for people to have an expectation of a certain degree of policing services in the high-tech crime environment just as they have a degree of certainty of such services in the real world.

There are well-recognised hurdles for us to overcome to help bring about this sense of security. Not the least is the difficulty that high-tech crimes, particularly Internet crimes, are often international and multijurisdictional in nature. The Australian High Tech Crime Centre is well placed to assist Australian law enforcement in that regard. Hosted by the Australian Federal Police, the centre makes use of the AFP's extensive international liaison officer network.

In addition, the centre is establishing strong links with like-minded institutions overseas such as the UK's National Hi-Tech Crime Unit and the FBI's Cybercrime Division. We have had an officer exchange program running with both these institutions so far. Domestically, we have national agreements in place between agencies which have started to address how we will fight high-tech crime nationally. The high level of support for a national effort is best illustrated by those who constitute my board of management—all Australian police commissioners, and the NZ police commissioner as an observer.

The investigation of high-tech crime relies upon the assistance of private sector organisations perhaps more than any traditional crime, because the Internet is owned by these organisations. We are working with key owners of the Internet infrastructure to try to address the issue of how we can better lawfully obtain information to fight crimes affecting Australians. The centre has also commenced negotiations with key Australian industries to work out partnership arrangements in order to more effectively share data on matters of national information infrastructure protection and to address chronic high-tech crime affecting the industries as a whole. To date, we have had a very positive reception.

Lastly, we see a strong need for education and prevention programs which reduce the likelihood of victimisation from the use of technology. The centre is in active discussions with other government agencies as well as with industry in looking for opportunities to contribute. On an operational note, today the committee may ask questions relating to current operations. If such questions arise, I will seek leave of the committee to answer those questions in camera.

CHAIR—Firstly, Mr MacGibbon, there is a lot of support for your organisation in the states, and some kind words are being said, so that is good. There is also the view that we really need to have one centre to effectively look at cybercrime around Australia. That recommendation has been made in both Sydney and Melbourne. What is your view? Some people are suggesting that, if such an organisation existed, it should be yours. How feasible is that and what capabilities would need to be added if you were to take a truly national role in that regard?

Federal Agent MacGibbon—Certainly, it is heartening to know that people are saying positive things about us. We recognise that these are very early days for us. Australian law enforcement agencies and police and justice ministers agreed to the formation of the centre in November last year. As I said, it is heartening to know that in the short time between the establishment phase and now we have not managed to blot our copybook too much.

The Internet is an interesting body to try to put law enforcement resources into. I mentioned in my opening statement that the international nature of it makes it difficult for us in many respects—and, I think, the cross-jurisdictional nature within Australia. You can have a high-tech crime centre anywhere in Australia. Because of the virtual nature of the crime we are looking at, a centre based in Canberra is a reasonable proposition. We believe we can add positive aspects to the broader Australian law enforcement contributions to this crime type. Equally, we know that

each jurisdiction has to maintain its own capability. They are the ones who hear about a range of these crimes that we will not hear of. They are the ones who are expected to react in a very timely fashion when these crimes occur. I believe there is a case for a national centre with a strong international linkage that relies upon the cooperation and goodwill of our partner agencies. I would like to think that the High Tech Crime Centre, in its current form, is a positive contribution to law enforcement.

As far as resources go, it is difficult to say. I heard a question to your previous witness in relation to policing chat rooms or being online in chat rooms. There are hundreds of thousands there. How many resources do we put online in order to put in a policing presence? What type of automation can we use to create a policing presence, to filter for activities in a lawful way and to create a profile for law enforcement so that people are at least aware? The analogy I use is that it is equivalent to driving a marked police car through a bad neighbourhood at the same time as having detectives in there and surveillance officers who are conducting covert inquiries. We need to do a similar thing on the Internet. We could always use more resources, but at the moment, with our current projected range of staff, we are reasonably confident about being able to deliver the types of capabilities we have mentioned in our submission to you.

CHAIR—In response to some of the issues that have been raised by other people, what do you think, in regard to your last comment, is the feasibility of having regular police audits of the chat rooms, for the same reason you said the marked car would drive through—or unmarked, in this case? People knowing that that is happening on a regular basis may cause some caution to be exercised by those who think it is a total free market.

Federal Agent MacGibbon—Sure. I think there is benefit in the internationally cooperative side of things that may go part-way towards answering your question—key strategic alliances with other agencies that are online, both domestically and internationally. The FBI run a significant program called Innocent Images. The US customs service maintain quite a significant online presence. If we are talking about, for example, child sex offenders online, the BKA in Germany are quite aggressive in a proper lawful sense, the UK maintain very good operations, and New Zealand as well. So the key perhaps is to work more closely than we are now, and we are certainly tracking towards a much higher degree of cooperation in how we coordinate our efforts. There may well be—I have been asking this question lately—some technological ways we could actually create a policing presence that overtly goes into chat rooms. But I think that, just because of the sheer scale of the Internet, any effective law enforcement in that sense is very hard. There are monitored chat rooms, of course, and they provide a certain degree of protection for people in there, in that the people who provide that facility for the chat room monitor it. That can, I guess, be good and bad, but in the child-safe ones that should be a good thing.

CHAIR—One of the comments the deputy chair made in the last session was on the need to focus on the ones who were putting children at risk; that to try and monitor everything and so on is not possible but that we could put a hard focus on the ones who are the major problems.

Federal Agent MacGibbon—If you have to focus resources, children at risk have to be the priority in a chat room environment because it is well recognised that that is where the child sex offenders will go to find and then groom victims. Again, I think the key is proper international targeting, ensuring that when a partner agency offshore find someone in Australia that is appearing to groom children they have a single point of entry into the Australian law

enforcement system so that we can act on that appropriately. Equally, we should be able to go offshore and act through our partners against people who are trawling for or trying to find Australian victims.

The question was raised with the previous witness as to how you can tell when someone is being flirtatious—I am not trying to make it sound like it is a proper relationship; I mean someone who is satisfying their predilections just through dirty talk with children as opposed to someone who is actually willing to either travel or arrange for the child to travel for sexual purposes. It is a difficult one. We are actually consulting with psychologists now to work out whether there are key phrases or other activities that people may engage in. We are also dealing with offshore and domestic agencies to try to see if there is a certain set. I know the FBI maintain that there are certain characteristics of people online that they look for. Our aim is to try and find out what the world's best practice is and be a player within that constellation of agencies.

CHAIR—Good. When someone is convicted of a child sex offence or is brought in for questioning over a child sex offence, is their personal computer taken as well to check out what pornographic child imagery they store and connections they might have had with chat rooms et cetera?

Federal Agent MacGibbon—All of the legislation in Australia at the moment is state and territory legislation. The Commonwealth has flagged under changes to the Telecommunications Act certain aspects to do with child pornography and other sex matters online. That does come down to the individual operating activities of the state and territory police.

CHAIR—Do you think that should happen, though?

Federal Agent MacGibbon—I think across the board with law enforcement there is a recognition that computers generally, in all crime types, can play a key role in evidence gathering. It would be a rare day these days that law enforcement would not pay attention, particularly in sex offences cases, to what is stored in home computers. That depends on the law and what you need to do to seize that. In some states you can seize it, presuming it has evidence. Under a Commonwealth search warrant, we would need to show that there are certain things on that computer that justify its seizure. It should be nominated, and generally is, in the conditions of a warrant that we are seeking any form of electronic storage device. That is generally for all crimes, and I believe that child sex investigators pay particular attention to electronically stored evidence.

CHAIR—I do not know if you were there when our first witness talked to us about the issue that the most likely person to offend is one who has been convicted before. There was some suggestion that a person who had been convicted of a child sex offence should have a monitoring device on their computer as part of their parole period or even going longer than that. Has that got merit?

Federal Agent MacGibbon—I believe there have been some conditions placed on computer offenders in other crime types to not have access to computers. You can do that, but I think there is always the prospect of people being able to work around those types of bans. If you place it on a home computer, there are wireless devices that you can access—Internet cafes and the like—

that people could use to go around it. It is not the same as having an ankle bracelet that lets you know when they are online.

Mr SERCOMBE—It could still be a breach of a parole condition, which has significant consequences.

Federal Agent MacGibbon—Certainly. It would be one trigger for showing a breach. The amazing thing about the Internet, of course, is its accessibility—the multitude of ways that you can access it.

CHAIR—Have you found that Internet cafes are where a lot of the child sex offenders go online?

Federal Agent MacGibbon—It would be hard to give a generic answer to that. We find across the board, when we are talking about high-tech crimes, that Internet cafes play a significant role because of the increased anonymity associated with their use. It would be hard for me to comment on individual crime types, but I would suspect that perhaps more of that would be done at home, based on the nature of the offender. Certainly Internet cafes, from an investigation point of view, present unique challenges to us, because in order to obtain the evidence of what a person has been doing, in a long-term investigation, we actually need to go to that Internet cafe, execute a search warrant and seize the data. This, of course, makes our intentions and our activities known to, possibly, the offender. If it is a longer term job, it is very hard for us to gain that type of evidence.

Mr SERCOMBE—Going back to some of the international liaison issues you spoke about, I think it was the German police agency you referred to, the BKA, that adopts a very aggressive approach—I think that was the expression you used—to sexual predators using the Net. Could you perhaps give us a little amplification of what you characterise as aggressive on their part and what is done by them that may not be done by other police forces?

I will now go to the question of international agencies and back to this theme of trying to get an understanding of the profile of the sort of person who is likely to be a serious threat to children. I am aware that, for example, the FBI particularly—I think at one of their places in Virginia; I cannot think of the name of it but it was made famous in one of those corny movies—

Federal Agent MacGibbon—Quantico?

Mr SERCOMBE—It is where they have the VICAP technology. Are you aware of serious work being done elsewhere that we can draw on in Australia to get a better understanding of the potential for someone who is acting in an Internet chat room in what the community might regard as a slightly bizarre way to progress through the system to become a very serious threat to children, possibly even a killer of children? Are you able to point us in the direction of serious work being done in that respect that enables some predictions to be made about where resources ought to go?

Federal Agent MacGibbon—In relation to the BKA, my interpretation is that they probably just have a high number of officers online. I guess the aggressive side is that they have been quite adept at passing that information offshore, particularly to the US where so much of the

Internet is hosted, or so much of the traffic goes through. I spent three years in Washington prior to taking up this position, and I know that the BKA was very regularly in contact with US agencies, providing data in relation to potential offenders that they had encountered online.

There are two aspects to this. There is the legislative aspect and the fact that they would have the legislation in place to look at a range of potential sex offences, and there are really two types to that. One is the child pornography side and the other is the grooming aspect. In relation to the grooming aspect, to the second part of your question about Quantico, as we speak we are conducting a project looking at the world's best practice in how we identify people online who are potentially the real sex offenders—again, I say the word 'real'—

Mr SERCOMBE—Serious.

Federal Agent MacGibbon—and who are talking to a child in a situation that may lead to physical contact and to sex offences in the physical world. We are in active discussions. I have had an officer in London for the last couple of weeks talking to the UK National High-Tech Crime Unit. One of the key aspects of his visit was in relation to their way of filtering. The Internet means that you have hundreds of thousands of potential offenders in these chat rooms, and you need to know how to filter it down to a reasonable number so that you can have the level of suspicion or belief about it that lets you do the extra, more intrusive investigative aspects—how you locate that offender and how you look at engaging them in the physical world. That same officer will be travelling to the US in the first stage of that program in, I think, another week to talk again to, particularly, those involved in the Innocent Images program, which is the FBI's main child sex investigations area and which also maintains a proactive online presence, posing as children online and engaging people in conversation.

The US provides an interesting illustration for us on how you have to be careful about the legislative aspects. They have a thing called a 'travelling offence' there. There is a federal law about crossing a state boundary in order to commit a serious offence. That legislation comes from the unique history of US law enforcement, where they have, obviously, many more states and a much more fragmented law enforcement system than exists in Australia. So the travelling offence is the main offence that they would use in relation to child sex offenders. Getting on a Greyhound bus and travelling to Baltimore from Washington is crossing a state boundary and therefore, if an offender is going there for the purpose of having sex with what they believe would be a minor, is an offence in itself.

It is a good question that you ask and one that we hope to give the committee answers to in a couple of months time. One of the benefits of being a new centre is that we can devote resources to things that others for a long time would have thought was a good thing to do. Because we can come to this part of crime with a reasonably clean slate, we have the advantage of trying to conduct these national and international surveys to give us, hopefully—at least as far as when the survey is completed—the edge in our online investigations.

Mr SERCOMBE—Do you have the resources at present to do this task satisfactorily?

Federal Agent MacGibbon—Yes, we do, I believe. It is a matter of prioritisation, but certainly online offences against children is a key priority within the states and territories and, as

a national policing organisation, it is imperative that we devote a significant percentage of our resources to that activity, even if that means that we drop off on other investigations.

CHAIR—There was some question in another jurisdiction that information was slow to come to us, that Europeans swap information within the EU and that information flowed freely in the United States but that we were at the end of the line. Do you think that is a fair comment?

Federal Agent MacGibbon—I do not think it is a fair representation of how Australian law enforcement is regarded offshore. Australia, given our relatively small population and certain obscurity geographically, has a very high profile not just amongst the law enforcement agencies of Western countries. We really do have a good reputation that we can use to leverage investigations conducted offshore. But I will say that we recognise the need to move more forcefully in relation to child sex offences online. One of the key priorities for the centre is to create stronger links with key units.

We leverage off the backbone of the AFP's international network, which is a surprisingly large network for a country of our size and for an agency of the AFP's size. That gives us a centre of reach that we could not hope to have if we were a stand-alone organisation. I do not think the flow of information is necessarily slow. The important thing is to make sure that those countries know that we are interested and are committed to actually acting on information. We recognise that we can always improve on that. Whilst the centre is only three weeks old, we have already started the process of looking at what information has come through in the past and how we could better act on that in the future to ensure that we do what I think the public has a right to expect—that is, treat offences against children as a very high priority.

CHAIR—Do you think we are sufficiently ahead of the game in terms of technology? Would the equipment, techniques and methods that we are using mirror what is being carried out in overseas law enforcement agencies? Is particular technology that could lead us on to the next phase in terms of crime detection on the Internet being talked about?

Federal Agent MacGibbon—Technology, including software, is one aspect of this activity. There are the resources that you devote physically. I have been asked several times if we have the people to do it. The answer is that we could always do with more. Please do not misinterpret my comment that we will address this problem; there is no doubt that we would always welcome more staff online. It is a combination of technologies, including hardware and software; the practices that you actually use when you are online; the number of people you have; and the relationships you have with other agencies offshore and domestically. If any one of those falls down, I believe you have wasted your money on the others.

So, to answer your question in relation to technology, I think we have the right hardware and we are always willing to look at new software to understand how that can contribute to our efforts. I will stress again that being three weeks old formally gives us the ability to look at these problems with a fresh view. I think technologically we are on the right track. As a percentage of what we have available to us at the moment, we certainly regard staff resources as our highest priority. International and national arrangements are getting better by the day. I think they started off at a very high level anyway. I do not want people to get the impression that there is no agreement between states and territories and that there is no agreement internationally. There are

very strong agreements. One of our objectives is to make sure that they are even stronger and more able to cope with volume crimes.

CHAIR—I understand that you have not had a long time in which to analyse various cases with regard to Internet cafes. Is it more appropriate in terms of the seizure of hard drives and so on to look at the various Internet accounts that are being activated that may be used in Internet cafes?

Federal Agent MacGibbon—Certainly, Chair. What I can do—and what I am doing, by the way—is draw upon the knowledge of the AFP's high-tech crime unit. That now forms the core of the High Tech Crime Centre. In our defence, that federal unit looked specifically at key Commonwealth legislation and so the child sex side of things was not really our business—apart from possibly assisting in the distribution of intelligence.

Internet cafes do pose a problem for us, and you raise a very interesting point in relation to the actual Internet accounts people use there. The unfortunate problem is that the bulk of those accounts are free Web based email accounts that a person can create with very few details, if any. Often the only thing recorded is the IP number from the machine that they were sitting at at the time of raising the account—the equivalent of a phone number or a street address, once you look up that IP number, of where the person was—or which ISP was used to establish that free Web based IP.

It is a real difficulty for us because the law we use in order to investigate or to require information from Internet service providers is the Telecommunications Act, specifically section 282, where we reasonably say that the information is necessary for us and we compel them to provide evidence. The evidence is not content and it is not real-time; it is things like the IP numbers and what is called packet header information in relation to what a person has done online—not so that you know what they have written necessarily, but it gives you an indication of what the person has been doing.

The difficulty is that, while an Internet service provider can provide that capability to an Australian—I hope I am making sense here, by the way—sitting behind a computer in Australia, the servers for that service are more than likely somewhere in the US, and how do we then use our section 282 notice to get that Internet service provider to give us the information? Our interpretation of the Telecommunications Act is that they are carriage service providers under the terms of the Telecommunications Act and therefore they should provide us that information. But their head office in California, for example, may not concur with our interpretation, and the question is whether Australian law can go into the fine state of California and convince them they should provide us that data. They often have corporate offices located in Australia and we are in discussions with the free major ISPs that are commonly used—not because the ISPs themselves are problematic but because they do provide that flexibility of not being tied into a home account—to see whether there are ways that we can apply Australian laws to those ISPs.

CHAIR—In opening up an account normally, you often have to provide three pieces of identity; but with this, like in other areas, it seems that all the rules go out the window.

Federal Agent MacGibbon—There is no 'know your customer rule' in relation to it. The only data that is captured by those ISPs is data that helps them do their business, which is a

logical amount of data to capture. In the case of a free ISP, the amount of information they need to do their business is very little because they make their money through other means: advertising and the like.

Mr SERCOMBE—Hotmail being the most obvious.

Federal Agent MacGibbon—Hotmail being one, yes. Certainly Hotmail figures quite prominently in our investigations—not because Microsoft is a bad company but because it provides an excellent product that can be used by people anywhere in the world. It provides a pretty high level of anonymity, and that is very good for a criminal and very bad for a law enforcement officer.

Mr SERCOMBE—Not bad for Bill Gates.

Senator HUTCHINS—I want to go to the issue of child sex offenders. I hope I have got it right in my mind; I did appreciate your opening remarks about trying to demystify it and about these being real crimes that can be dealt with physically. Is there potential for you to cross the boundaries in terms of privacy? Also, is there any requirement for you to get any authorisation to go and look at people's accounts, as the chairman was talking about?

Federal Agent MacGibbon—Yes, there are. We are certainly very conscious of privacy for all people on the Internet. We would contend that our actions are to try to protect the privacy and integrity of the Internet from an Australian perspective and to try to reduce the number of victims that there are, and, when someone becomes a victim, to try and address that through the criminal justice process.

You are right. Being online gives us an opportunity to come across privacy issues that we may not have come across in the physical world. If we were in a chat room and people were having an active conversation, they would be aware that someone else is in that room who is also taking part or reading that conversation. We have controlled operations certificates for undercover activities that allow us to breach laws in a controlled fashion and for a stated objective, which we obviously take very seriously.

As far as obtaining data from ISPs and telecommunications providers, we provide them with a section 282 certificate, which only officers of a certain rank or in a certain position can sign, as a way of restricting the potential for excessive breaches of privacy. We are also exempt under the privacy laws for legitimate law enforcement investigations. There is a range of protections that we have for breaching privacy in a very controlled fashion. By the nature of the investigations that we are conducting, we are also philosophically trying to uphold people's privacy. It is of serious concern to us.

Senator HUTCHINS—If you suspected my having a shed full of pirated CDs or something like that, you would give me a warrant and then go in and search the shed. Do you have to advise people that you are watching them on the Internet? Do they have to be notified, for example, that 'from 10 a.m. on 21 July and prior to that we are going to go through your records'? Do they actually know that they are being watched?

Federal Agent MacGibbon—If I understand the question, the simple answer is no, but there is that range of protections that the parliament has put in place through various forms of legislation to ensure that the types of privacy breaches are done in a controlled fashion. If we were to conduct, for example, under the Cybercrime Act—

Senator HUTCHINS—It is a bit like a stake-out, is it?

Federal Agent MacGibbon—It is not dissimilar to physical surveillance where we do not actually need to let people know that they are under surveillance. What will happen of course if someone is arrested and charged is that, under the disclosure provisions, people will know the extent of law enforcement activity, which is probably the more appropriate time for them to know than prior to overt acts. For example, with a Crimes Act search warrant, but using the cybercrime provisions, we can access data. If we execute a search warrant on a computer in this room that was networked and we believed there was evidence in another location, we can access that evidence through the computer within the property that we were executing the warrant on. We then need to go to reasonable steps to let the person who owned the server or whatever else that we had accessed know that we had accessed that data. There are some provisions in place. In a sense, it is the equivalent of an occupier's notice for a search warrant, but giving it to a person away from the actual jurisdiction or from the actual warrant.

Senator HUTCHINS—On Friday we heard evidence from a chap in relation to a number of computer viruses. I think they were W32 Bugbear and Code Red, as well as a few others. He said that people had been charged and convicted for only a few of the viruses that had been put into the system. I suppose my question follows what I asked Professor Grabosky: are we essentially just being reactive? Can we be proactive in preventing that sort of crime in the future or is it something that we have just got to expect?

Mr Klein—I might give you some ideas on that. It is very difficult to do on the technology side. It would be akin to stopping someone putting something dangerous into Sydney Harbour. It is a type of malicious program that essentially anyone can create. They can find the information on how to do it, do so, and then propagate it. In terms of investigations, there are things that we will do to investigate that. We might analyse the kind of program it is, try to identify the author and things like that; but it is something that is very difficult to prevent. Although a computer virus has this notion of being a virus that spreads around, propagates and does terrible things, essentially it is just a program. It is a piece of computer programming just like every other program in the world, and it is very hard to stop people creating those things and propagating them.

Federal Agent MacGibbon—The Cybercrime Act criminalises the authoring of these codes and their malicious distribution, as opposed to your computer getting infected and then going about the process of reinfecting everyone in your address book. We have had some discussions with key private industry players, in the virus sense, to see if there are ways that we could move from a law enforcement perspective against people who are believed to be more malicious or if there are any ways for us to identify the authors. In time, we would hope that we could be slightly more proactive, but I think what Mr Klein said there shows that the problems associated with trying to track down the authors can certainly be pretty onerous.

Senator HUTCHINS—Our inquiry is concentrating on three points. In your opinion, is there anything regarding legislation that needs to be addressed? Do we need to think about going about something in a different way or adding to or subtracting from something?

Federal Agent MacGibbon—Rather than just try to suggest legislation, if I answer the question in a manner that highlights where we see our problems then perhaps the committee can determine whether or not there are actual legislative ways to solve these problems.

Senator HUTCHINS—That is fine.

Federal Agent MacGibbon—There is the question of obtaining data from ISPs and carriers as we move to an ever more global world and how we serve lawful Australian processes on people. There have been recent examples in Australia where questions have been raised in relation to offshore hosting of facilities. A large corporate received publicity recently over some gambling advertising on their web site. The answer was that it was hosted offshore, but they were still held accountable by the public and the government for what was there. There was the civil case of Gutnick, where a server offshore affected a person in Melbourne and therefore there was the question of how litigation was to be carried out.

Where the locus of the offence is and where the victims are et cetera are really interesting questions that the Internet has created for us. From a law enforcement point of view, we simply would like to have the capability to conduct inquiries in a lawful fashion that protects people's privacy as best as possible but allows us to investigate the crimes that the public expect us to investigate, whether it involves servers offshore or in Australia. We can conduct those inquiries through other means, through partnering with offshore agencies, but they often require an offence to have occurred in that country before they can exercise their own lawful mechanisms for accessing data.

If we were talking about the United States, for example, and a person who was using Hotmail to communicate with another person in Australia, unless there was an offender or a victim in the United States the mere fact that the communication had gone through the US would not be enough to trigger the US law enforcement's assistance for us, because under their law there is no real law broken. If there were any way of addressing that, we would obviously welcome it. I think there have been very strong moves in the Cybercrime Act, for example, to strengthen key aspects of Internet criminality, and we are quite satisfied on the legislative front that we have reasonable tools available to us to conduct inquiries—but it is very early days for us as yet.

Senator HUTCHINS—Thank you.

CHAIR—That was very interesting.

Senator GREIG—My recollection is that the Commonwealth cybercrime legislation is about two years old.

Federal Agent MacGibbon—I think so, yes.

Senator GREIG—Have there been any convictions under that act since its implementation?

Federal Agent MacGibbon—No, I do not think there have been any convictions. We have arrested a few people under those provisions. Those cases are still before the courts, so it is obviously improper for me to comment on those particular matters. If we were looking at reasons for the delay, a lot of that had to do with upskilling the appropriate people to conduct the inquiries from the federal side of things. Of course, the next important hurdle is being able to successfully reach a stage where one is able to lay charges.

Internet investigations have a volatility that some others may not have. I am not saying that it is the hardest crime in the world to investigate but certainly, while we will receive a number of complaints, whether the actual evidence that we need in order to help build a brief is there is often quite a problem for us. Part of what we are doing is to try to help the industry that owns most of the servers, if they are victims, to capture the right type of data, to make sure that the right logging mechanisms are turned on and to make sure that they handle that material in a manner that is forensically sound and that allows us to then present it before a criminal court. We also try to encourage industry to report matters to us, as we recognise that as being an issue. So I think the short answer to your question is no.

Senator GREIG—Is your organisation, or any similar Australian organisation or authority, empowered in any way to use entrapment—to be an agent provocateur—in terms of trying to discreetly solicit people to come forward with their crimes over the Internet?

Federal Agent MacGibbon—We have provisions for controlled operations of ours to break certain laws but entrapment is not one of those processes. Looking specifically at child sex offences, when the law enforcement agency goes online in a covert capacity, they do so as a passive child that does not actually make any type of suggestive move, so there is no concept of entrapment there. What they present is a parry to every advancement and they do not actually lead that person on. Looking at the breaching of certain laws, as I say, there are controlled operation certificates, but entrapment is not one of the processes that we would employ.

Senator GREIG—In regard to the area of high-tech crime—and in a minute I will ask why you differentiate between high-tech crime and cybercrime—do you feel that Australian businesses are generally aware of security, privacy implications and the level of vulnerability to or opportunity for these kinds of crimes? In comparison to other western countries, are Australian businesses up to speed with necessary protective mechanisms for trying to prevent theft and fraud online?

Federal Agent MacGibbon—The AFP participated with AusCERT and other law enforcement agencies in the production of the *Australian computer crime and security survey*, which was released in May—and I can get copies for you if the committee wishes. The survey shows that corporations are spending more money on IT security aspects but it also shows certain generic vulnerabilities within some industries. For example, there is a belief that, if you run virus protection software, you are protected against all forms of malicious computer activities. There should be firewalls, intrusion detection systems and importantly, from a corporations point of view, a policy on computer security so that you do not use a disk to import something from outside the organisation and around the normal protections that the organisation has.

Along with Standards Australia and the Attorney-General's Department, we have funded the production of a computer forensics first-responders type guide for industry which is an evidence collection guide that I believe is being released for public comment in the next couple of weeks in an effort to work with industry on how they may start protecting themselves and how to gather the information that we need to effectively prosecute. As I mentioned earlier, the problem is often that, while we know the attack or incident has happened, the evidence for us to proceed is just not there.

I think that, on the whole, there is recognition within industry that they need to protect people's data and that the way to do that is through effective IT security policies and IT security systems. But IT security is a specialised field. It is no longer just the job of the person who understands computers in an office but is a specialised job where you upload the correct patches in the right type of order in a timely fashion and where you are across the new exploits as they occur. Nick is an IT expert, so I should throw this to him. IT security is always going to be one step behind the leading edge of criminality just by the sheer nature of it. You can only build defences against what you know of. The key is defence in depth and the right types of policies in place to ensure that the defensive computer systems you have in place are not worked around by someone like me giving my password out and allowing someone to take over the system.

Mr Klein—In terms of the landscape of Australian businesses, I would say that, generally, businesses are aware of what needs to be done, and they do the right things in terms of putting in the right procedures, the right policies and having the right security mechanisms. Security is not a simple thing; it is very difficult, and it involves not only the technology but the process aspect. You could have bulletproof systems but, if there is a flaw in the way that the business processes operate, it is still possible to commit crimes using those systems. The other thing, as Alastair said, is that there is certainly every opportunity available to Australian businesses to get the right level of security. There are very sound risk management and information security standards in Australia. There are certainly many organisations that can provide assistance. Companies that engage in statutory audits will have some sort of IT security component to those to make sure that there is enough assurance in the systems. There are more products and services out there than there ever have been for securing systems, so the opportunities are certainly there.

There are always going to be companies which, through lack of understanding or exposure to these kinds of issues, are slightly behind. But, as I said, there are more opportunities than ever before to get the right level of security. In terms of the part that we can play, we have already talked a bit about education and cooperation, and I think that we will continue to help raise awareness and provide education.

Federal Agent MacGibbon—Industry is a pretty big spectrum, and there are key industries that are obviously well protected. I think that comes from their bricks and mortar days of having bars on windows and bigger locks on doors. You find that with banking and telecommunications computers the companies that own them spend more effort in relation to IT security matters than some other companies that have never really seen themselves as holding data that is worth while. But, to a criminal, identity data—credit card and home address details—might well be what they are after. Whatever the particular person wants might be available on a range of systems that are much less protected than those in the banking sector and the telecommunications companies. In fact, the same data might be held by someone else for a different purpose. It is all about finding the weakness in the Net.

Senator GREIG—So the prize is not necessarily dollars and cents but information?

Federal Agent MacGibbon—Information equals dollars and cents, in many respects. Rather than going after the bank, for example, you might make money in some other way, through another type of fraud where you have taken over a person's identity and obtained or stolen their money.

Senator GREIG—The end goal may not necessarily be money, either.

Federal Agent MacGibbon—No.

Senator GREIG—Information could be for other purposes.

Federal Agent MacGibbon—It could be anything ranging from industrial espionage and competitive information through to a criminal who is sick and tired of police and other government agencies that can keep track of them knowing who they are. Certainly technology provides an increased capability for criminals to hide their identities and to obtain new ones. The unfortunate aspect is that they are often legitimate people's identities who become victims in their own right.

Senator GREIG—You made a point of saying in the beginning that you draw a distinction between cybercrime and high-tech crime. Why do you do that? What are the political and linguistic differences between those two which you feel are important?

Federal Agent MacGibbon—Apart from the fact that we are called a high-tech crime centre, the real reason is that we are not concentrating just on the Internet—and cyber is usually referred to as the Internet. We are looking at the misuse of technology in a more holistic sense. The danger is that we will miss other exploits or other criminal activities that fall outside the strict definition of the Internet. At the moment, we have an investigation that relates to the abuse of technology that is not Internet related but is equally significant to the community. I have some difficulties talking about it in an open fashion but it goes to the functioning of that particular sector and how it impacts upon individuals—and possibly misuse by criminals on a whole range of fronts. We do not want to limit ourselves to just the Internet, while recognising that the Internet will form the backbone of a whole range of those activities—even things like telephony, with the move to IP telephone systems rather than switch systems, are becoming part of the Internet. That is the reason for drawing that distinction.

Senator GREIG—Thank you.

CHAIR—Before we finish up, is banking and credit card fraud on the increase?

Federal Agent MacGibbon—Statistics in relation to high-tech crimes are problematic in Australia at the moment, in our opinion. We think there is a good opportunity with the formation of the centre to start addressing it. We sat in on Professor Grabosky's testimony and he was asked questions in relation to how we were capturing this data. We see the formation of the centre as a good opportunity to start gathering baseline information to give you a credible answer. What I would say in relation to it from an anecdotal side is that, as technology proliferates and there is increased access to technology by individuals, you would have to

surmise that there is increased opportunity for crime. From what we can see in the banking frauds that we have come across—again, in very general terms—it is the end users that are compromised rather than the banking system itself. We have no problems with banking sector computers. The difficulty is that you are asking millions of people using their own systems to get access to the banks, and that is where the problem may lie. Indeed, while my credit card and the details of it might be well protected by the bank, if I allow it to go out of sight there is always the possibility that someone could take the data on that card. No matter how good the banking systems are, there is always a chance that they could be misused by a criminal.

CHAIR—Are you getting good cooperation from the private sector?

Federal Agent MacGibbon—So far it is very heartening. I cannot stress enough the extraordinarily positive response we have had from industry. We have met with several key sectors and put to them propositions in relation to providing data that they might not ordinarily provide to police, for a range of reasons—perhaps because they thought we were not interested in the past. I do not think that is true, but there is a perception that police were not interested. It may have been because of its complexity or an ability to handle it in-house and change the system slightly to accommodate it or to weed it out in that fashion. We have had a very positive reception.

The ultimate goal of the High Tech Crime Centre—taking into account privacy and trade practices restrictions, which we are very conscious of—would be to have key private sector national information infrastructure representatives in the centre itself to give us lawful access—because it would only ever be done in that fashion—thus reducing some of the bureaucratic hurdles that may occur in trying to access data lawfully. Perhaps more importantly, it would help us to get the expertise that is housed in the private sector—expertise that as a law enforcement agency we can never hope to retain in the right type of numbers and the right type of currency that you need to investigate some of the high-end crimes. So there has been a very heartening and positive response to date from industry and there is, from the letters that we have received subsequent to meetings, a strong commitment by them to cooperate with us in terms of operations and potential collocation of staff, which I think would benefit the Australian public.

CHAIR—My final question concerns the proportion of high-tech crime which you see as part of organised crime and the proportion which involves individual activities.

Federal Agent MacGibbon—That is a very difficult question. It could be either. We certainly do see traditional organised crime groups using technology, whether it is the technology to help them commit their traditional crimes or a new crime that they want to get in on. We have seen that and I believe we will continue to see it. But the Internet also offers individuals the capability to conduct crime that they may not otherwise have had the capability to do before. I think the real key is that it has diversified the potential criminal population quite significantly, and that in itself is a law enforcement challenge as to how you respond to the atypical crime.

I might add that we might regard them as individuals because they are not physically meeting, but they may well have some way of swapping data and sharing computer exploits. We have seen instances, for example, on the intellectual property front where there have been people geographically separated—never physically meeting—who work in a very syndicated fashion, a traditional organised crime fashion, to break the protections that are put on there by software

manufacturers. They then distribute that virtually to people who have different roles in that organisation, and conduct a criminal enterprise in all senses of the word except that they are not physically together down at the pub. It is a very different way to look at crime.

CHAIR—Thank you for your input, which has been excellent and helped us draw out a number of key factors in relation to our inquiry. This is the last day of our inquiry. Thank you for the briefing that you gave us before in terms of your centre, which was useful. I appreciate the time and effort you put into today's hearing.

[11.12 a.m.]

MELICK, Mr Aziz Gregory (Private capacity)

CHAIR—I call the committee to order and resume this public meeting of the parliamentary Joint Committee on the Australian Crime Commission. The committee is examining recent trends in practices and methods of cybercrime with a particular reference to, one, child pornography and associated paedophile activity; two, banking, including credit card fraud and money laundering; and, three, threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime.

I welcome Mr Greg Melick. As you know, the committee would prefer all evidence to be given in public, but if at any stage you wish to have your evidence taken in camera then please request that of the committee and we will consider your request. I now invite you to make an opening statement and then we will proceed with questions.

Mr Melick—Thank you, Chair. What I want to do today is just bring to the committee's attention what I consider to be some of the major jurisdictional problems involved in dealing with crimes over the Internet. Most of what I have to say is not new. I have been raising some of the issues with parliamentary committees for over seven years. I am frustrated that not a lot has occurred, although the High Tech Crime Centre is definitely a step in the right direction.

I have distributed a very basic paper that I wrote in 1999, so I will not go through most of the issues raised there. It is a very simple paper, but it highlights the underlying problem. It is interesting to note that in 1997—and I was not aware of it when I wrote that paper—Janet Reno, when Attorney-General of the United States, addressed G8 countries in relation to cybercrime and indicated four steps that had to be taken. They are steps that I agree with. The first is the enactment of sufficient laws to appropriately criminalise computer and telecommunications abuses. The second is the commitment of personnel and resources to combat high-tech and computer related crime. The third is an improvement in global abilities to locate and identify those who abuse information technologies. The fourth is the development of improved regimes for collecting and sharing evidence of these crimes so that those responsible can be brought to justice.

I have to say two things from the outset: firstly, it cannot be done without cooperation between law enforcement and private industry—and I think that point has been made to the committee before; and, secondly, it cannot be done without appropriate cooperation between nations. We are not going to get that cooperation unless we are prepared to enter into dialogue with those nations at a very senior level, at the ambassador or cabinet minister level. There is not much point in sending somebody from the Australian Attorney-General's Department to attend a conference and bring back information because, at the pace at which we are going, it is going to take far too long.

Part of the problem at the moment is the law. It is very hard to get a coherent system of responsibility in relation to the Internet. The law development in Australia is still piecemeal. Macquarie Bank and Berg was a case in New South Wales where Justice Caroline Simpson decided not to take jurisdiction because she took the view that it would be almost impossible to enforce her orders. The opposite approach was taken by Justice Hedigan, in Victoria, in Gutnick's case. He conferred jurisdiction for defamation on an Australian court for material that was published in the United States. But one has to be a little careful about that because the information was only available in Australia to those people who subscribed to a service. So it was not necessarily freely available information; it was just downloaded onto the Web and extracted. I happen to think the rationale in Gutnick's case is the way to go, but we have to be a little more proactive than that.

In the United States in 1952 they enacted section 1343 of the criminal code, which is what they call the wire fraud provisions, which made it an offence to use any part of the telecommunications system to commit a fraudulent offence or part of a fraudulent offence. What that did was federalise a lot of crimes which otherwise would have been state crimes, and that led to a significant increase in federal law enforcement agencies and prosecutors dealing with the matters. I suggested a similar sort of provision in Australia in relation to the Telecommunications Act, to give federal jurisdiction for anybody who commits any part of any crime using the telecommunications system. It was rejected out of hand because of the cost, the intrusion of the Commonwealth into state areas and the concern that the necessary increase would have to be to both the Federal Police and the DPP's office. But until we do something like that, we are going to continue to have problems.

The United Kingdom has enacted that, if an act or result occurs in the United Kingdom, then it gains jurisdiction, which overcomes some of the problems. But until we start enacting appropriate laws, both as to jurisdiction and preservation of evidence, we are not going to get very far. In 1996 I suggested that everybody who used an Internet account should have to go through a 100-point check, the same as if opening a bank account. Industry thought the idea was laughable and it had amazing problems, because if we do it in isolation it does not do much about the people in the rest of the world who have access to accounts over there. But I would like to note a few statistics. When I raised this the first time, Australia had something like 600,000 Internet users. We now have seven million. In 2000 the United Kingdom had six million; in 2002 it had 10 million. In the United States alone from 1996 to 1997—that is, from the beginning of 1996 to the end of 1997—Internet users went from 40 to 100 million. People may suggest that the horse has well and truly bolted, but if one does not start doing something about it sooner rather than later we are going to have further problems down the line. France, as far as we are aware, is the only country that has done anything about it. About two years ago it enacted such provisions.

A short-term fix which would make life a lot easier would be to do away with free Internet accounts such as AOL and Hotmail and matters such as that, because if Internet accounts are not free, people have to pay by credit card, and the vast majority of people who use credit cards have provided appropriate information when obtaining the credit cards and that gives law enforcement some starting point. I am aware, of course, that any serious criminal is going to have access to false credit cards or credit cards with false details, but at least it is a start.

In 1997 a survey in the United States found that 62 per cent of people who applied for Internet addresses supplied false information in at least one material particular. A lot of it was concern for privacy rather than a desire to conduct illegal activities, but it is disconcerting to note that even if you can trace an Internet communication back to a user name it is not going to get you very far.

That leads me to the next area of problems, which is tracing. If I send an email from here to California, it may go through up to 14 servers. Some of it may be done by telecommunications lines, some by satellite links. Some of the service providers may have sophisticated electronic equipment enabling the retention and storage of data. Some may have old mechanically operated switches—although they are falling by the wayside now—which either do not have provision for the storage of data or, if they do, do not count very much data. In the United States they have the provision to hit an Internet provider with a preservation order, and they must maintain records for a certain period of time, in relation to the area of transactions that are subject to the preservation order. We have no such law in Australia, let alone a requirement for Internet service providers to keep records for any particular period of time.

There has to be international cooperation between governments to force Internet service providers to comply with certain protocols; that is, to actually record data, to keep it—in other words, to preserve it—and to supply it to law enforcement agencies when requested. That leads, of course, to jurisdictional problems. If a terrorist act occurs somewhere in the United States and interferes with an Australian air traffic control flight system, which causes aircraft to misread heights above runways and crash, what do we do about it? If it comes from the United States, we have probably got to trace it back to an Internet service provider over there—if we can. It may have started with that Internet service provider, or it may have been channelled through it. If the attack occurs in Australia during the day, the likelihood is that it is at night in the United States and there is going to be nobody there. Do we have the right to then start inquiring down the line and intruding into their service providers' records without first getting a formal extradition request? To reverse the situation, if there is a mutual systems request which comes from the United States to Australia, the death penalty is applicable in the United States, so do we provide the information which relates to a terrorist activity?

All the usual problems about mutual assistance rear their ugly head with the Internet. When you note that some mutual assistance requests take anywhere between nine months and nine years to implement, you realise that the horse is going to have well and truly bolted. My view is that we have got to start being proactive, to get involved with G8 countries and the European Union—and I recognise the fact that we actually adopted their draft legislation in part of our Cybercrime Act—to make sure that there is appropriate international cooperation and to not put things off for another seven to 10 years, because in the meantime the pace at which these matters are developing is going to make it far harder for us to catch up.

One of the matters that continually frustrates me is that people say, 'We do not have the technical competence to enforce a lot of the laws you're talking about bringing in.' My view is: get the legislation in there, enforce it where you can and hope that technology catches up to enable you to enforce it. But in the meantime, if you have not got the legislative cover, you are really frustrating law enforcement agencies trying to go about their job.

I think that is about all I wanted to say by way of opening, although Senator Greig asked a question about entrapment before. There are no special laws for entrapment in relation to the

Internet; it is just the general law in Australia, which is basically subject to certain constraints, such as the preservation of the right to silence. You can entrap people. You can have the basic example of a policeman leaving a whole lot of television sets in the boot of a car when he knows a known criminal is going to be walking by, and hoping he is tempted to take the television sets. The other extent is going out and actively encouraging him to go out of his way to steal the sets. The law stops somewhere between the two as to what is appropriate and what is not appropriate. I have not looked at this law for a while but, in the last four or five years, there have been two High Court cases—Pavic and Swaffield—which talk about those sorts of issues and when you can encroach on the right to silence by the use of entrapment. If the committee wants any work done on that, I can probably drag up some notes and send you some information.

CHAIR—Thank you very much for that; it was as interesting and provocative as usual. Firstly, I would like to talk to you about the general issue of coordination and to what extent the High Tech Crime Centre, which gave evidence before you, is meeting the need for coordination of cybercrime investigation within the country. It would seem that the other jurisdictions were complimentary about the work being carried out by this new unit, although its track record is not long as it has only recently been established. Do you think that is a hopeful sign for coordination on a national basis? I would agree with you that there are many players.

Mr Melick—The trouble is that there are too many players and no overarching coordinator. I was involved in a National Office for the Information Economy committee dealing with a lot of these issues. We spent three years examining our navels and got virtually nowhere. There was not the political imperative to push it. Organisations such as the then NCA, the Australian Federal Police and state police forces were just too busy, and will always be too busy, to take a strategic view about this sort of matter. We tried to take a strategic view. We did not have the funding or the resources to do it, and we could not get government interested.

I would have thought that, now terrorism is rearing its ugly head all over the world and is fairly popular politically as a vehicle for all sorts of things, we probably should use that as a vehicle to establish a committee on this. Probably all you need is an Internet ambassador, so to speak—somebody who has the ability to advise government on overarching policy and strategic direction and can liaise at that sort of level with other countries and carry some sort of weight. I have found that, in your operative law enforcement, even at commissioner level, you can have all sorts of good ideas but it takes a lot to translate those ideas into the political reality.

CHAIR—Because of your involvement in the former NCA, do you think it is more appropriate that the High Tech Crime Centre handle these issues or should it be the newly formed Australian Crime Commission? It seems that, in quite a few of these, it is a bit hard to determine to what extent organised crime is involved—with banking fraud, perhaps, and credit card fraud to a certain extent, whereas sex offences seem to be more an individual case.

Mr Melick—You might have internecine disputes whichever way you go. I do not know whether either of those organisations really has the expertise to deal with the overarching strategic issues, and that is the problem. I am not being critical—I think what they are doing is extremely good and the people who have sourced it are very good—but they are not the people who have the necessary legal knowledge, diplomatic knowledge or overarching understanding of the international problems to solve the major problem—that is, giving themselves the legislative cover to do what they want. I really think there has to be something above both of those

organisations that will take information from all of the organisations in Australia, both state and federal, and will express its concern or give detailed policy direction or advice to the federal government. This matter has to be coordinated federally. It is federal, not state; there is no question about that.

CHAIR—I think that is an interesting point because the High Tech Crime Centre is more operations driven rather policy driven.

Mr Melick—They are likely to be handling the tactical and operational areas, not the strategic.

CHAIR—Currently that exists, I presume, with Attorney-General's.

Mr Melick—I do not know if it exists anywhere. We tried to get it going. The NOIE committees tended to deal with a lot of what I call commercial broadbanding issues and other such matters, and law enforcement issues were tagged on as a necessary evil. I think most people consider that it is all too hard and we cannot do it by ourselves and if America is not going to do it what is the point? My view is that, unless a few countries start doing it—and France has—and we start pushing it at the G8 level, at the European Union level and in ASEAN and places like that, we are not going to get very far. We have other organisations such as FATF, the Financial Action Task Force, and it is also in their interests to make sure that this sort of stuff is coordinated. At the moment there are a lot of well-meaning bodies at relatively high levels operating all over the place but within Australia they are not even being coordinated.

Mr SERCOMBE—Could you give us some further information about the experience in France?

Mr Melick—I left the NCA at the beginning of 2000. I have presented one or two papers internationally since then, but I really have not had the time or the resources to keep on top of what is going on. I think it has been a bit like the take-down notices in Australia, in that it is honoured more in the breach than in the enforcement. But France took the view that somebody had to make a start, and it was prepared to do it. As I said, I know the Internet service providers were very anti it, because it meant that they had to have a physical location for people to turn up to to open an Internet account. They could not do it virtually, and they thought that they were going to lose a lot of business. As to what has happened, I am afraid I cannot take it any further. There was a major conference in 2000 where a lot of countries were getting together to discuss these issues. I recommended that somebody went to it, but I am not sure what happened. I do not know whether or not Australia sent anybody. That is the sort of thing we should be doing to get this information back.

Mr SERCOMBE—One would think that, given France's position in the European Union, if they have taken some initiatives in this respect then there is more likely to be a general European application so that it potentially assumes a bit of critical mass.

Mr Melick—I think it was regarded by a lot of the other European countries as a flash of Gallic madness. Once again, the problem was that until some other people started doing it, people thought, 'What's the use, as long as you have AOL and Hotmail online free of charge, so any French citizen can get a free Internet account in the United States without supplying identity

details?' Sooner rather than later the large corporations like Microsoft and other providers of these free services have to be brought to heel and told, 'Look, it is a great idea to have free speech, but the cost is too high. We have to at least be able to know who is saying things.'

CHAIR—You mentioned the UK, but they do not have the states to deal with, as we do here. Quite often you have national bodies there that coordinate, which makes it helpful.

Mr Melick—Just about anything on the Internet in Australia has to use a telecommunications system, which is federal, and that overcomes it. That is why the American government brought in the wire fraud legislation in 1952. I believe they have now strengthened that to incorporate things other than fraud, including terrorism.

CHAIR—I find your idea of the 100-point check for service providers interesting. It ties in with the weakness we see at the moment, which is just free access.

Mr Melick—The committee found it very interesting when I said it to them in 1996, Chair, and nothing has happened since then.

CHAIR—This is a very proactive committee.

Senator HUTCHINS—The Australian Crime Commission has suggested that the kinds of powers to issue cyberwarrants under section 25A of the ASIO Act could be made available to it. To what extent can this kind of surveillance of Internet activity be dealt with under existing legislation, to what extent do you think such a facility is necessary and what alternatives might there be?

Mr Melick—Since the ASIO Act came in, I am afraid that I am not aware of the full extent of the current legislation. Your biggest problem with any warrant in relation to Internet traffic is knowing where to look. It is very easy if you are getting it at either end, but it is almost impossible to get something in the middle unless you have an end point or a start point. As far as I am aware, there is no basis upon which the Australian Crime Commission could do a general search in the ether to extract information. I think they would need that sort of power, but it is a bit like looking for a needle in the haystack.

CHAIR—Section 25A would provide you with that access, but it has to be in the national interest.

Mr Melick—That is what I am saying—section 25A, I understand, is an ASIO provision.

CHAIR—It is. It must be seen as being in Australia's national interest. Some people think it is too draconian to use in this area.

Mr Melick—Most of your relevant data and evidence for law enforcement purposes will come from computer hard drives. Once you get that information, you then should be able to go to the various Internet providers to get the preserved data to get your evidentiary trail to lead you to the perpetrator. That is the way I would see it working at the moment. To randomly try to pluck something out of the ether and interpret it to see what is going on will be almost impossible. You also have the other problems of encryption and steganography.

Senator GREIG—Mr Melick, you are advocating the abolition, or at least the regulation of, Hotmail accounts or free accounts—be it Yahoo or whatever. I am struggling to understand where that fits into the concepts that the committee has been looking at, in particular theft and fraud and child pornography. It seems to me that if a paedophile were to be soliciting children or trying to access children, they would do that without any recourse to a Hotmail account or a Yahoo account. They are not logging into a chat room through that. The point of reference, the point of identity, would be with the ISP. So it would be with the registering with the Internet company. That would be the point at which you may be required to submit information as to who you were and where you lived—not with a Yahoo account or a Hotmail account. Equally, with theft and fraud, if somebody were engaging in cybercrime online, they would not necessarily be doing it with a free account. The only exception I can think of is the Nigerian scam, which is still running hot. Most seem to be Hotmail account based. But if somebody were engaging in, say, credit card fraud, I am not quite sure where a free account scenario would come into that.

Mr Melick—They use an account. They have to use an account to do it.

Senator GREIG—But not to go into a chat room.

Mr Melick—So how do they go into the chat room?

Senator GREIG—Let me paint a picture. Let us say you have a paedophile who has an email account. So they are online; they are with an ISP—let us call it 'oz.net'. I am just making that name up.

Mr Melick—So the chat room is online?

Senator GREIG—Yes. So they go into a chat room. Let us say they go into Disneyland Chat, where they can reasonably expect to find children. There is no reference whatsoever in their discussion in that chat room to any free account.

Mr Melick—No, because they just use an identity which they use on the Internet.

Senator GREIG—If the authorities were trying to geographically locate that person, it is irrelevant whether or not they had a free account. What they really need to do is try and locate the ISP through which that person is registered at point of origin, their home point, with the view to perhaps identifying where they were, at a geographical residential address.

Mr Melick—They have to have an Internet identity before they go into a chat room and use it.

Senator GREIG—But I am right, though, aren't I, in saying that that would not be circumvented by having a free account?

Mr Melick—I see where you are coming from; sorry. What I am concerned about is that, before you actually get recognised by an Internet service provider, whether it be via an account or through a chat room, you should have a provable identity. One way to overcome that problem is to get rid of the free accounts. You should at least do it through a credit card; otherwise you can say to an ISP provider: 'You cannot take information from somebody before you establish

their identity.' The best way to establish identity is to have an Internet address. The Internet address should be tied to a 100-point check. This will take years.

Senator GREIG—I follow that but my understanding, my own experience, having signed up through two different ISPs in Perth, is that once you do that they provide you with your email account, and the suffix of your email account is generally the name of the organisation and the name of the ISP you have joined.

Mr Melick—Yes.

Senator GREIG—It is not a question of going to an ISP with a view to signing up an account and their providing a free account with a Hotmail address. As I understand it, you could not do that.

Mr Melick—I do not think I follow you. I may be wrong but, as far as I am aware, you cannot go into a chat room unless you have some Internet identifier. You have to be known to somebody. In fact, you have to be known to an ISP provider; you have to have an email address—hang on; I had better be careful about that.

Senator GREIG—I am not sure that is the case. I could walk into an Internet cafe in Civic this afternoon and log into any number—thousands—of chat rooms and there would be no identification of me or, I suspect, the cafe concerned.

Mr Melick—How do they get back to you?

Senator GREIG—Who is 'they'—the authorities?

Mr Melick—No, the people you are trying to contact.

Senator GREIG—The cafe itself would already be online—

Mr Melick—I understand that.

Senator GREIG—I could go into an Internet cafe in Civic and log into the chat room of Ford cars and talk about Ford cars all afternoon, but nobody monitoring that scenario would have any knowledge or access to any email account that I may or may not have, whether or not it was an open account.

Mr Melick—That is right, so long as you are online, but once you get off-line there is no one way they can come back to you. It will not overcome that transit situation; I understand that. I am sorry; we were at cross-purposes. But that also means that, if you want to establish a communication with somebody, the only way you can do it is by going back into it through an anonymous chat room. They can never come back to you because they have no email address to come back to.

CHAIR—I think, Senator Greig, that that is quite an interesting point you are making, but it does highlight the fact that it is an imperfect situation: whenever you try to get a handle on it, it slips and moves, and there is a problem in all of this area in trying to get some controls on it. But

I think, as the deputy chair pointed out earlier in the day, that the main concern is to get to the hard core of the groups that are the offenders, and that is why I think that at the bottom line there is merit in having registration of ISP providers and so on.

Mr Melick—You could take that to the next step: before you can use a chat room you have to be recognised by an ISP, and the only way you can be recognised is by having an email address.

CHAIR—Like the provision of identity going into an Internet café?

Mr Melick—I thought it would be simpler if you could not even use the Internet system unless you have some form of electronic identification such as your email address or whatever, although you have to be careful because if everybody knows the email address they can forge it. That does become a problem, because if everybody knows somebody else's email address they could use that. They would have to have a code for the email address as well. Every time you lift up a stone, there is something else underneath it. But, although it is an extremely difficult problem, that does not mean that we should not try to tackle it.

CHAIR—I agree.

Mr SERCOMBE—I was interested in your referring to the American initiative in having a capacity to order an ISP to preserve material. Are you able to give us further details on that? Is that possible for a civil action as well as for a criminal matter?

Mr Melick—No, I am almost certain it is only criminal, and there are only certain people who can issue them. I am not sure whether I have any notes on that. It has been in for several years now.

Mr SERCOMBE—So the effect is that the FBI could, presumably, by showing due cause—having a reasonable suspicion or whatever is the equivalent American expression—take an action to get a court to order an ISP to preserve material.

Mr Melick—Yes, and there is a specific form, like a warrant form, that they get which lays out information. I can dig that up and send it through to the committee. I think it was legislated in 1997 or 1998. It has been around for a while now.

CHAIR—I suppose the question I want to pursue is really that one of the points system. At the bottom line, raising some of the issues that we have, do you still think it is feasible and workable?

Mr Melick—It was in 1996. It gets harder every week that goes by, and it would take many years to catch up with the people who have already registered. The answer is that I think you have to discuss it at the appropriate level, at one of these committees, to find out whether or not some of the large payers are prepared to get involved—bearing in mind that there are always going to be rogue states that, for commercial reasons, want to provide an Internet haven in the same way that some provide a banking haven. The point is that it will certainly cut out a lot of the casual crime, or the people who get involved casually. Your hardcore people are always going to be difficult to track down, and you will have to get them by using traditional policing methods.

I think it is a matter that has to be seriously raised at the international level. There has to be a commitment from our government's point of view to say, 'We are prepared to look at this seriously; who is going to be in it with us?' and let them come up with reasons why they do not want to do it. America will probably say, 'We have 120 million people online. We do not want to do it because that is too big a backlog.' As to how many of those are foreign, I do not know, bearing in mind that people all over the world use Hotmail and AOL online in matters such as that.

CHAIR—I think one of the key things coming out of your evidence today is this need for greater coordination both within the country and offshore and at a sufficiently high level so that we have access to the changes that are occurring.

Mr Melick—I think somebody should be concentrating on that and on nothing else. If you say to Mick Keelty, 'You do it,' he may immediately be distracted by another terrorist attack—or, worse still, by parliamentarians involved in travel rorts.

CHAIR—What jurisdictions are you aware of that have such a group?

Mr Melick—The Americans have a very high-level group which is quite extensive and is having a lot of money being spent on it. I met two of the people who head it up at a conference in Charleston in December.

CHAIR—And what is it called?

Mr Melick—I knew you would ask that; I am trying to think of it now. I might have a note of it here.

CHAIR—Perhaps you can come back to us with that. It is just so that we can follow through and perhaps get some more information on what they do. If we are going to make any recommendations in that area, it would be useful to have a model. Did you say that the UK has a similar one?

Mr Melick—No. Funnily enough, the Serious Fraud Office took a bit of a lead on that for commercial reasons, led by Rosalind Wright, but since the terrorist concerns it has become more centralised. The United Nations has been doing it, but the trouble with everything the United Nations does is that it tends to get bogged down in politics. I have a list of some of the things that are happening. I will contact Chris Paynter, in the United States, who was involved with that group and get some information.

CHAIR—If you could provide us with that information, that would be very useful. Thank you very much for coming here today. It has been very interesting. Any other post-attendance inspiration that comes to you can be forwarded to our very efficient secretary.

Mr Melick—There is an article in a 1999 G4 journal which I think you might find useful. I will send that to you.

CHAIR—Thank you.

[11.55 a.m.]

INMAN, Mr Keith, Director, Electronic Enforcement, Australian Securities and Investments Commission

CHAIR—I call the committee to order and declare reconvened this public meeting of the parliamentary Joint Committee on the Australian Crime Commission. The committee is examining recent trends and practices and methods of cybercrime, with particular reference to, firstly, child pornography and associated paedophile activity; secondly, banking, including credit card fraud and money laundering; and, thirdly, threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime.

I now welcome our next witness, Mr Keith Inman of ASIC. The committee prefers all evidence to be given in public, but if at any stage you wish to go in camera could you please advise the committee and we will consider it and then, hopefully, proceed. I invite you now to make your opening comments and then we will follow that with questions.

Mr Inman—It has been two years and three months since ASIC presented evidence to the Joint Committee on the National Crime Authority during the committee's inquiry into the law enforcement implications of new technology. I thought it might be useful if I made a number of opening observations by reflecting on some of ASIC's comments back then and where we find ourselves today.

In April 2001 ASIC pointed to its recent experiences, indicating a significant and rapid up-take of the use and the abuse of the Internet technologies. At that time our Electronic Enforcement Unit was on target to deal with 200 matters in the 2001 calendar year. Our experience so far this year indicates that the unit will be dealing with some 300 matters by year end. In our 2001 submission ASIC had raised the suggestion of the need for additional powers where our enforcement experiences had identified a number of gaps in our capabilities. Since that date, the Cybercrime Act amendments have flowed through into the Crimes Act and provided a number of additional powers. Although those amendments did not address all of ASIC's concerns, they have certainly helped with respect to obtaining digital evidence during the execution of Crimes Act search warrants.

Back then, we made the observation that international cooperation was going to be vital in the fight against cybercrime, and that has certainly come true. It is ASIC's opinion that currently the greatest threats to consumers and investors arise from overseas destinations. The majority of the mass-marketed online scams that ASIC comes across are sourced to overseas based services or sources. This does not, however, mean that Australia is free from such conduct, and ASIC continues to investigate a steady flow of matters involving the abuse of the Internet delivery channels. Spam was then, and remains now, a significant concern for ASIC as the main delivery channel for scams and deceptions. The committee is, I am sure, aware of the recent in-depth review of spam by the National Office for the Information Economy, NOIE. Without wanting to consume all the available time by reiterating the analysis and findings contained within the

NOIE report, ASIC would like to register its support for, in particular, recommendation No. 8, that a new offence of using a carriage service to commit any Commonwealth offence should be considered further by the relevant policy departments, for all the reasons contained within the NOIE report.

One of the reasons that spam is such a threat, of course, has been the widespread uptake and use of email in our society and in business. This move towards the use of email over and above traditional paper based correspondence continues to create operational difficulties for ASIC. The lack of clarity under the law as to when an email can be seized as a piece of correspondence under ASIC's various access powers and as to when it must be viewed as a communication subject to telecommunications interception powers—which are not applicable to ASIC—continues to frustrate some of our investigations. ASIC views this as a critical impediment and a significant dilution of its enforcement capability. Cooperation between Australian law enforcement agencies was high on our agenda—

CHAIR—I will just stop you there. Are you saying that you would like some legislative strength in order to be able to take control of the emails?

Mr Inman—If I may, I will seek your indulgence for just a moment and put to you a hypothetical scenario. Let us put this into a boardroom environment. As a result of some financial presentations to the board, you as a member of the board suddenly realised that there was an opportunity for you to commit a fraud against the company. You wrote some instructions on a piece of paper to your fellow board member and passed the paper across in an envelope. The instructions were: 'There's an opportunity here; if you take steps 1 and 2, I'll take step 3 and I'll split the proceeds 50 per cent.' You slip that to your colleague on the board, but your colleague on the board happened to get up during a break in the board meeting and walked away. At all times, ASIC access powers, under the regime we currently have, could gain access to that communication—as you are writing it, once you have folded it and put it in the envelope, and while it is sitting on the desk waiting for your fellow board member to come back and read it. If in fact you had decided to send that by email or, maybe, SMS from your mobile phone to your colleague's mobile phone, the proposition at the moment is that that could well require a telecommunications interception warrant, and therefore that information, or that conspiracy evidence, is not available to ASIC. It is in that context that I make my statement.

Cooperation between Australian law enforcement agencies was high on our agenda in 2001 and remains so today. At that time, ASIC drew attention to the findings of the report of the Research Group into the Law Enforcement Implications of Electronic Commerce—known by the acronym of RGEC—and the work of its successor, the Action Group into the Law Enforcement Implications of Electronic Commerce, the AGEC. Our evidence made particular reference to the recommendations from both the RGEC and the AGEC for the creation of a national centre for expertise in high-tech crime. ASIC has taken comfort from the recent creation of the Australian High Tech Crime Centre and will be giving direct support to assist in the establishment of the new group.

Making mention of multiagency cooperation is an apt way of bringing me to my next observation from our submission in 2001, relating to record keeping by Internet service providers. This topic was of particular interest to the committee at that time and has remained a crucial topic for law enforcement and national security agencies since. In many respects, the

previous inquiry became a catalyst for a new level of Internet industry and agency cooperation. In developing its final submission to the inquiry, the AGEC commenced a round of discussions with the Internet Industry Association's newly created cybercrime task force. The IIA and agencies recognised a commonality of interest between industry and government in prevention, detection and investigation of online fraud and other criminal activity and threats to national security and information infrastructure generally.

The Internet continues to deliver enormous efficiency benefits to business and facilitates the free flow of information and ideas. Confidence of consumers and business in the use of information infrastructure as a means to do business and to communicate is dependent upon that infrastructure being safe, secure from unwarranted intrusions upon personal privacy and commercial confidentiality, and reliable. Safety, security and reliability of the Internet are dependent upon early detection of criminal activity that might undermine achievement of these objectives. This, however, requires a balancing of such fundamental rights as the right of individuals to privacy of communications and the right of individuals to be protected against criminal activities.

This commonality of interest led to a suggestion by the IIA that it would be willing to examine the creation of a cybercrime code of practice to provide guidance for its members. The AGEC was asked to provide a mechanism for national consultation with law enforcement and national security agencies. The project was jointly sponsored by the e-security coordination group and the Australasian Police Commissioners E-Crime Steering Committee.

The draft code has been developed recognising the cost of online fraud and other criminal activity and the cost of its prevention, detection and investigation. Online fraud imposes a substantial cost on ISPs, which is ultimately borne by Internet users. The code will endeavour to set clear procedures for cooperation between ISPs, law enforcement agencies and national security agencies in an effort to ensure that all these costs are minimised and equitably allocated. The code is also an important part of the Internet industry's initiatives to address end-users' concerns that they may have risks in dealing online. Those initiatives include the industry's education as to the availability and use of more secure methods of payment, virus protection software and personal firewalls.

The AGEC worked jointly with the Australian Centre for Policing Research, using existing consultation networks in the form of the ACA's law enforcement advisory committee and the ACPR's Australasian Computer Crime Managers Group to research the issues and to reach a truly national agreement and consensus on the advice provided to the IIA. The IIA has also consulted with the Commonwealth Privacy Commissioner on the content of the draft code. I have been advised by the IIA that the code includes a requirement that ISPs who are not already subject to the Privacy Act may only subscribe to the code if the IIA has been provided with written evidence that the ISP has elected to be treated as an organisation in accordance with section 6EA of the Privacy Act. Agency advice to the IIA on the code was finalised in March this year, and I have been informed that the IIA will be releasing the code as a consultation draft this week. Without prejudging the final outcome of the IIA's consultation on the code, I must record my appreciation for the hard work put in by more than 20 officers for multiple agencies over the past two years and the commitment of the members of the Internet Industry Association's cybercrime task force.

My last comment on the IIA initiative will be an attempt to convey the general feeling of agencies involved in this consultation over the last two years. In providing advice to the IIA, the agencies analysed what was important or critical to a successful Internet based investigation. What eventually makes its way into the code will be a decision of the IIA. After all, it is their code and for their members. Although the final draft will not address all of the needs articulated by agencies, we acknowledge that there has been a genuine attempt to accommodate those needs balanced against the IIA's cost and privacy considerations. To that extent, agencies are willing to support the implementation of the code as a positive step forward in ensuring a safe and secure electronic environment for all. The IIA has additionally committed to an ongoing process to ensure that the code remains relevant over time.

I will finish my opening statement by making the briefest of comments on a trend that was foreseen in the AGEC report previously mentioned. The report pointed out that improvements in technologies would lead to greater levels of identity theft and false identities. I would like to confirm that ASIC investigations are now coming across more examples of the use of false identities in matters relevant to the Corporations Act—information we will be feeding into AUSTRAC's recently announced research project into identity theft. That concludes my opening statement.

CHAIR—Thanks very much. That gave us quite a bit of food for thought, Mr Inman. Quite often at the end of presentations and at the end of questioning, we ask what witnesses recommend to the committee, but I will put it at the beginning as there are obviously a whole lot of areas that ASIC is concerned about in relation to cybercrime and the need for legislative changes, codes of practice et cetera. What would you like to see in terms of this committee's recommendation in the areas that affect you and cybercrime?

Mr Inman—Rather than start with a wish list, I think it might be useful to try to overlay a strategic framework of the issues. I am aware that there have been two recent studies over the past three or four years that have resulted in the creation of a strategic framework to look at these issues, including the work that was done by the Research Group into the Law Enforcement Implications of Electronic Commerce—the RGEC—and the Police Commissioners E-Crime Steering Committee. Their work has also resulted in a similar strategic framework, and there is much crossover and commonality between those.

If I were to answer your question by highlighting some of that commonality, there are two areas that I could suggest need to be worked on in the future. I would put them under the headings of environmental strategies and capability strategies. I will deal with environmental strategies first. This is very much the classic crime prevention idea that police services have been working with for many decades. Under environmental strategies for industry, we can look towards the continued need to raise awareness and foster best practices for a risk management approach towards e-security. It is very much a 'bars on the windows', 'locks on the doors' approach, but in the modern environment.

CHAIR—Through a general awareness campaign per se? You are talking about self-regulation there.

Mr Inman—It is.

CHAIR—So lifting the awareness as part of an education campaign?

Mr Inman—I am very conscious of the government's approach to the support of the growth of e-commerce, and self-regulation is certainly the preferred option. There is much that has already been done and still some yet to be done over the next two to three years. Our experience has been that the big end of town takes this issue very seriously and expends a certain amount of resources in ensuring that its doors are locked and its windows are barred. I think we need to ensure that all of the financial industry intermediaries and players treat it similarly. We also need to promote the development of the appropriate skill sets through consultation with universities to continue the work that has been started in the last year and a half with the creation of appropriate degrees aimed at ensuring that we have a steady supply of trained professionals in the future years. There is still a gap—

CHAIR—Trained in what?

Mr Inman—It is so hard to expect that a general degree in IT would be sufficient to impart all the necessary specialisation needed to provide good, sound electronic security advice for any company or for the industry in a general sense. I think in the last 18 months we have seen a number of universities move towards the creation of specific degrees geared towards producing e-security graduates. It is that type of initiative that I am suggesting we need to continue to support.

With regard to the environmental strategies and moving from industry to consumers themselves, members of the public, there is clearly still significant work that needs to be done on raising consumer awareness. A committee member has already mentioned that the Nigerian letters remain the bane of everybody's life. Even after several years of education, it is clear that they still lead to victims. The message still has to be got across. As long as the Nigerian scams remain profitable, that is a good indicator that we have not got the message across as much as we need to.

We also need to support the work of industry in raising the awareness of their own clients—for instance, the Internet service providers—and the IIA's work in educating its clients about ensuring that they are secure at home, that they have virus protection and that they consider the utility of firewalls and some of the filtering software packages that are around for the protection of their children. As far as environmental strategies go overall, a tripartite approach is by far the best, where industry works with its clients, government works with industry and government works with clients to promulgate all of those good ideas and sensible strategies.

With regard to the capability strategies, that really defines tools and powers. For us, I think there is still some work that needs to be done on filling those gaps that have appeared as we have moved from the off-line paper based world to the electronic environment. I mentioned emails, which is by far my most topical example of that. Not only do we identify those gaps and seek solutions to them, but we should also be conscious of our opportunities to identify and apply the very technologies that are causing us frustrations. ASIC has fairly recently entered into a joint research project with one of the cooperative research centres to research the development of new technologies for classifying webpages so that we can proactively identify scams as soon as they appear on the Internet. Our partners in that research program, the Capital Markets CRC, describe it as Australia's largest language technology research project. That is certainly an example of

where we can try to apply, for our own benefit, the very technologies that are frustrating us. I think agencies need to continue to look for those opportunities.

Finally, under tools and powers, I think that significant steps forward have been taken with regard to training our own investigative enforcement staff. I think that the creation of the High Tech Crime Centre will go some way towards improving overall training standards for law enforcement and regulators nationally, and I look forward to that. I hope that in some way gives an answer to your big question.

CHAIR—That was pretty comprehensive—lots of fertile ground.

Senator HUTCHINS—On page 4 of your submission, Mr Inman, in the paragraph headed 'Any one of the above risk factors can jeopardise an enforcement outcome', it says at the end:

... it will routinely investigate matters that it cannot bring to a satisfactory outcome, because the trail simply dries up.

That seems to be a bit of an admission of—

Mr Inman—Gaps?

Senator HUTCHINS—not being a success.

Mr Inman—It is the reality.

Senator HUTCHINS—Can you expand on what you mean by that? Coming back to what the chairman asked about, is there anything in terms of legislation that we should consider so as to assist?

Mr Inman—First, I will explain that text a bit more. Ten years ago, the work of ASIC's Enforcement Directorate was very much paper based. If we investigated a contravention of the then Corporations Law, we would typically be dealing with lots and lots of boxes of documents, contracts and correspondence. Nowadays, not only do we deal with lots and lots of boxes of contracts and documentation; we also deal with large amounts of electronic data. When we take a proactive stance—that is, we try to identify an offence while it is still being perpetrated; a classic example is when a web site suddenly appears offering someone an investment, the content of which contravenes our legislation—we need to find out who is behind that. The types of material that we are dealing with when we do that are not paper based; they are very much logs—computer logs, network logs—and those types of things.

Our submission highlights the fact that, as a regulator undertaking an enforcement investigation, we rely very much on the logs and the computer records of non-government entities. That is where most of the information infrastructure is; it is in private hands. As we start to trace our way through that technology to the source of the offending material, we are dependent on companies, telecommunications carriers and Internet service providers to have logs operating.

At certain times, some of our investigations will come to an impasse. We will get to the stage where, for instance, an ISP or a company has not kept the necessary logs for us to be able to

identify with any degree of certainty the source of the offending content. In that context, in light of events in, say, the last three or four years, the only way that ASIC and other law enforcement agencies can seek to change that paradigm is to work with the industries and companies to raise awareness of the mutual benefits of keeping those logs.

For instance, I suggest in our submission that we do not ask companies to keep logs purely because it will help ASIC if and when we ever come to commence an investigation; we also point out that it is good e-security practice for themselves. If we cannot tell where the offending postings come from, it is very likely they cannot tell what their internal people are doing when they are meant to be at work pursuing the objectives of the company. Not only that, but if they do not keep appropriate logs they will find it more difficult to substantiate their claims if a business dispute ever arises involving an online transaction and they do not have the proper logs turned on. Does that help explain?

Senator HUTCHINS—Yes. Has it occurred that you have been doing an investigation into some aspect of a company's operations and that the police and all sorts of other bodies have also been investigating that? So far it seems to me that we have a lot of bodies coordinating things. Maybe this High Tech Crime Centre is the peak council, but it looks to me like there are a lot of people out there doing the same thing.

Mr Inman—The reason for that is that the technology is ubiquitous; it is across all facets of business and society. I do not think that we could ever hope that one government body would by itself solely be responsible for every misapplication of technology. Technology is just too perverse—sorry, pervasive. I am probably right in the first sense, too, on some occasions. For instance, in ASIC we now consider that it is a core competency of our investigators to understand the basic underlying infrastructure of the Internet and how to trace an email. That is a skill which 10 years ago would not have been on the drawing board, but we now come across it so regularly that our investigators need it, Australian Federal Police agents need it and Customs officers need it. Any government agency with an investigative role now needs that awareness. You cannot limit that to one individual agency.

However, for the reasons that Mr MacGibbon pointed out, having a centre of expertise such as the new High Tech Crime Centre really will help, because it should provide a focus for us to share to a greater extent and ensure that there is no overlap in training. But as far as operations are concerned, it is very rare—if it happens at all; and I cannot think of any examples over the last three years, say—that ASIC investigations stumble across investigations by the AFP or the New South Wales Police. What happens is that we tend to be aware very early on of other agencies' interests, and we coordinate our response accordingly.

Senator GREIG—You mentioned self-regulation a little earlier. I was not quite sure what it was that you were referring to. I understood it to be in terms of security and privacy mechanisms for industry and corporations—is that correct?

Mr Inman—My response was that, in the absence of any legislative powers, self-regulation is the only mechanism for agencies to seek to fill gaps in capabilities.

Senator GREIG—I heard you as saying, though, that your view was a preference for self-regulation.

Mr Inman—It is. And that flows through from policy decisions of the government. We fully agree with that.

Senator GREIG—Why? Why self-regulation as opposed to a parliamentary response that might set minimum standards in the first place?

Mr Inman—It would be inappropriate, I feel, to question the government's policy decision on that. I can say that it makes sense to ASIC that all of the participants in the new electronic environment—that means the public, consumers, industry and government—take responsibility to a certain degree to make it safe and secure. Therefore, self-regulation seems like an appropriate mechanism to help achieve that aim.

Senator GREIG—How does that compare in terms of comparable international jurisdictions? Are we witnessing self-regulation in comparable countries or is it more a parliamentary response?

Mr Inman—It is a very topical debate, and it has been in many jurisdictions for the last two or three years. We know that legislative suggestions have come to light in a number of European countries, but the debate continues. They are yet to result in any legislative amendments in any acts that we are aware of. As far as we are aware, the Internet Industry Association's cybercrime code of practice will be leading the way globally. We are yet to find another example of a code of practice that specifically addresses the areas that this draft code will. Again, I am not prejudging what the eventual outcome will be from the round of consultation, but in many respects that is world leading.

Senator GREIG—Is it a case of industry leading government or is it more cooperative?

Mr Inman—It is very cooperative. We have spent—as I alluded to earlier—two years, and other agencies have spent a lot of time and resources, providing detailed technical advice as to what our needs are. The Internet Industry Association has welcomed that. It might not meet all of our needs but, as I said earlier, there has been good faith shown by the Internet Industry Association, and there will be cost implications for the industry participants on this—there is no doubt about it. So they are taking their share of the load.

Mr SERCOMBE—It has been suggested to this committee—and we are not in the position yet to make a judgment about the particular matter, I do not think—that in the banking industry, for example, it is certainly technically feasible for the banks to provide a more secure framework for customers, in particular in the electronic banking environment. For a variety of reasons, of which cost may well be the most significant, the banks have not provided the levels of security that are feasible. At some point, presumably, the banks have made a commercial judgment about the losses—c'est la vie, I suppose. I just wonder whether you have got any comment on that in the context of your remarks about self-regulation. Obviously the directors or the management of a particular company in an industry like banking have got, in one view, a primary obligation to direct their commercial judgments to the commercial benefit of that entity. They are not obliged to take account of a broader set of policy requirements.

Mr Inman—I think that the experience, particularly in light of discussions and cooperative work that is under way with the critical information infrastructure protection strategy, shows that

financial industries in particular are willing to be engaged and do realise the potential harm that could be done to the industry if they did not protect their own assets. I have not come across a single example of a glaring gap in a financial institution's e-security framework not being addressed because the financial institute has said, 'We don't want to pay the money.'

Mr SERCOMBE—Do you use the adjective 'glaring' advisedly? You are aware of examples?

Mr Inman—No, I am not aware of any examples. Because I have been involved with a number of the vulnerability studies done in recent years, I know that the financial institutions take this obligation very seriously and spend quite a degree of funds on ensuring that they are secure.

Mr SERCOMBE—I have no doubt about that; I suppose it is the discussions about relativity and the trade-off—

Mr Inman—I will give you some credence in this particular line. For instance, you could imagine that the government might wish somebody's point of entry into their system, which is guarded by, say, a modem, to have significantly high encryption protection. The bank might say, 'That costs three times more than the next level down; therefore, for commercial reasons, we will apply only the next level down.' The reality is that that protects them adequately on their risk management scales. But that is all hypothetical; I have not come across an instance like that.

Mr SERCOMBE—In Melbourne this committee had its attention drawn to a set of circumstances that may no longer be applicable; we still have to establish this by further inquiry. A merchant allegedly found himself at an extraordinary disadvantage at having to bear huge costs associated with forgery because of the way in which the bank's arrangements for authorising and securing authorisations for transactions on credit cards over the phone were utilised. There is no real value going into the detail of that, particularly at this stage, but the committee has a specific example of some allegations by a person who on the face of it appears to be fairly credible about having been extraordinarily severely disadvantaged as a merchant because of the way the bank has secured the environment for payments in that situation.

Mr Inman—If that is an endemic problem, it would be of particular interest to ASIC. We have not seen any trends or sufficient information to believe that it is an endemic problem within the industry.

CHAIR—It was raised with the committee—in terms of self-regulation, it would appear, and the setting up of one's own standard of practice and so on. It came out of the UN report, didn't it, in terms of cybercrime? That is how I understand it. It does not matter. I understood it flowed from there.

Mr Inman—I think it is correct to say that both of these initiatives have occurred in parallel and are consistent.

CHAIR—Section 25A of the ASIO Act provides the ability to obtain evidence in critical areas—infrastructure and so on. It might be argued in the financial banking sector in which you operate that some of the threats to national security would warrant 25A. Do you have any views

on that? Do you envisage it being used? Would it, or does it, overcome the problems that you have outlined of gaining access to information?

Mr Inman—I will talk from an ASIC perspective but in respect of, potentially, the implication for the ACC, because it is the ACC which is the organisation established to deal with the organised crime threat, and I can see how that type of power would be up for consideration in that context. There is no doubt that, from time to time, organised crime does make use of the financial system, either to create ill-gotten gains or to launder the profits. It would seem to me that, if the ACC were investigating profit-making or money-laundering conduct of the nature described in some of the public submissions that I have seen, that type of covert capability would complement all of their other covert powers. It is not the type of capability that ASIC is asking for. You may have heard about the two different types of electronic crime: one which focuses on attacking the computer itself, and one where the computer is merely a tool. ASIC very much sits in where the computer is used as a tool. But I can see some of the hypothetical scenarios that are being put up in some of the public submissions, of where organised crime could seek to take advantage and attack computers. In those circumstances, if the criminals are remotely accessing computers, then maybe it makes sense that the organised crime investigative body investigating them may have a similar ability. But it is a philosophical stance only.

CHAIR—Is the question of search warrants a problem in this area? I notice it has been used in terms of the evidence.

Mr Inman—So far ASIC are not aware of any major problems. Search warrant access powers came under examination in recent times in a couple of matters, and we fared well. The recent amendments via the Cybercrime Act addressed many of our concerns about the execution of search warrants and the obtaining of digital evidence. We do not have any additional concerns to report.

CHAIR—What about the comments made by your former colleague Mr Melick in relation to the registration of ISPs? Do you think they have some merit?

Mr Inman—When we started talking to the Internet Industry Association, most of the agencies were of that view. The industry put forward a case that stated that the cost associated with that was impractical from their point of view. The agencies reached a compromise in many respects. We believe that, if the ISPs are aware of the incoming phone number by which their client is contacting them, that gives investigative agencies an ability to trace the source back to the suspect. So we are using that as a proxy for a 100-point identification system, say. As to whether or not that will be successful, time will tell. But agencies took comfort from that suggestion, and recent moves to ensure that Internet service providers have access to that type of information are, I think, a good step forward.

CHAIR—And have they?

Mr Inman—Yes, they have. DCITA may be the department to advise the committee on that. Based on the discussions I have had, I believe that information is now becoming available to Internet service providers.

CHAIR—So you are reasonably confident about that?

Mr Inman—Yes.

CHAIR—We will pursue that further, because obviously that involves a lot of the questions of security and so on. Are you seeing a significant increase in the general area of banking fraud and credit card fraud?

Mr Inman—I will start off by answering it this way: those types of offences are predominantly contraventions of the state crimes acts and generally the state police services are responsible for investigating them. ASIC's interest in those contraventions is very much from the consumer protection angle. Our interests along those lines are to ensure that financial institutions are aware of the threats, that they implement appropriate risk management strategies, that they provide clear instructions to their clients with regard to their obligations and the clients' liabilities in those circumstances and that they undertake the education of their clients as to safe practices. Having said that, there is no doubt that the arrival of the Internet technologies has provided new opportunities for people to commit new types of scams. The examples we have had in recent times of the spam email saying, 'This is a financial institution; please update your PIN,' is an example of that. Without spam and Internet technology, that crime would not occur.

The fact that we have seen reported in the press something like half a dozen of those matters in the last three of four months does not necessarily equate to a flood. To balance that up, I know, for example, that with regard to one of those matters involving a large Australian financial institution—and I do not think it warrants me mentioning their name, because there is no adverse connotation to this—they very quickly were able to identify the Australian connection, they worked with the New South Wales Police, and someone was arrested within three days of that spam email going out. I understand that person has been charged subsequently with deception.

I do not think we are seeing anecdotally a flood of these matters, but when they do occur it appears that the financial institutions, working with the police services, are able to protect themselves adequately and take recourse. It might be worth pointing out that we have actually cotrained some staff from that particular financial institution with our own investigators. We have also cosponsored some of their client education material. That does not mean that we can claim any of the kudos for their good work; I am sure that rests with the New South Wales Police.

Mr SERCOMBE—If we were to ask, 'Which bank?' we would be fairly close to the mark, wouldn't we? If it is the case I am thinking of, on the information we have the person who was arrested was a pretty low-level operator in the whole context of the exercise. The promoters of the whole exercise are overseas, and it is a bit equivalent in the drug trade to catching a mule at the airport and the people promoting the trade being untouchable. I am not sure we can take too much comfort from that example.

Mr Inman—I look at it in a slightly different way. I think the message that will go out is that, if you are silly enough to get involved with any overseas groups and you are the bunny in Australia, there is every chance you are going to end up in jail.

Mr SERCOMBE—I am not suggesting for one moment that that is not right. I am just saying that, in having some confidence about the capacity to deal with these matters, it would be much

more comforting if some of the promoters and the significant players were being hit, not some mule who has just been used for part of the onshore processing.

Mr Inman—I think that is right. I also think we can take some heart from the fact that they are overseas sources. The level of victimisation that anecdotally we appear to be suffering in Australia is well below that suffered by some of our overseas developed country brethren. For instance, the US Securities and Exchange Commission receives some 500 complaints daily about online abuses. ASIC is nowhere near that mark, and I think that is something we can take heart from.

CHAIR—What about credit card fraud?

Mr Inman—I am not informed enough to be able to give any view on that.

CHAIR—Fine. Finally, you talked about the ISPs being able to provide the phone numbers of those who are accessing the Internet. It would appear that quite a bit of the activities of a criminal nature using the Internet come from Internet cafes. How is that going to help us in trying to track people down?

Mr Inman—The Internet service providers will be able to speak for themselves, but representatives from ISPs have told me that they are less and less interested in allowing people to become clients when they log on from unsubstantiated points. I know of at least one large ISP who tells me that even though somebody can buy an account for cash, via a CD from a shop, the moment they want to log on they are required to contact the ISP and provide a contact number. If that is different to the information that their systems are telling them, they will not go ahead with the connection for the client. Their reason for that is that they have learnt that there is a large cost associated with those types of clients—they create more problems and more expense for them.

CHAIR—Thanks very much, Mr Inman; we appreciate your contribution today.

Proceedings suspended from 12.47 p.m. to 2.15 p.m.

GRAHAM, Ms Irene, Executive Director, Electronic Frontiers Australia Inc.

CHAIR—I reconvene this public meeting of the parliamentary Joint Committee on the Australian Crime Commission. The committee is examining recent trends in practices and methods of cybercrime, with particular reference to child pornography and associated paedophile activity; banking, including credit card fraud and money laundering; and threats to national critical infrastructure. When it reports, the committee wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime.

The committee welcomes our next witness. As you may be aware, the committee prefers all evidence to be given in public, but please make a request to the committee should you at some stage wish to go in camera. I now invite you to make your opening statement.

Ms Graham—We would like to thank the committee for the opportunity to present the views of Electronic Frontiers Australia today. As we have lodged a written submission, I will not go into detail about our concerns here, but I will make a few brief opening remarks. I appear today as an advocate for a balanced approach to law enforcement that takes individuals' privacy and other civil liberties into account. EFA recognises and supports the need to counter criminal use of the Internet. We are concerned, however, by the increasing prevalence of legislative proposals and laws concerning the Internet that fail to contain an appropriate balance between individuals' privacy and the legitimate needs of law enforcement agencies.

The federal parliament has long recognised the need for telecommunications privacy and the rights of individuals to communicate across public networks without undue or unauthorised scrutiny. Telecommunications interception has been treated as a serious matter, justified only in serious circumstances and requiring judicial oversight. However, in recent years restrictions in that area have been loosened and a number of proposals for combating crime have been seriously deficient. They would undermine important rights that exist to protect the innocent, without any evidence that the measures would have the intended impact on criminal activity. We are very concerned by the government's desire to permit government agencies to access the content of email, voicemail and SMS messages that are delayed in transit without a warrant of any description whatsoever. Also of concern are proposals for mandatory retention of transaction log records by Internet service providers just in case some of the information might be useful at some time in the future.

These proposals have the potential to result in it becoming lawful for government agencies to obtain a vast wealth of communication data without a judicial warrant. A requirement for ISP logging or monitoring would be tantamount to sanctioning mass surveillance and would be an infringement of the fundamental human rights of Internet users. It is also of concern that some existing laws prevent law-abiding Internet users from reporting criminal activity to law enforcement agencies and could result in victims of criminal activity being prosecuted. In that regard, for example, we have raised the problem of unsolicited and unintentional receipt via the Internet of material depicting child sexual abuse. This presents serious and frightening problems for Internet users: not only are they confronted with unwanted material, they also face the risk of criminal conviction for possession of material that came into their possession without their

knowledge and intent. Generally, recipients of this type of material suffer in silence because, if they report the criminal activity to law enforcement agencies, they risk being prosecuted for possession.

We consider there is an urgent need for review and reform of possession laws in a number of states and territories, to minimise the likelihood of Internet users being prosecuted for events that are beyond their control. An alternative way of achieving the same objective would be a carefully and thoughtfully formulated Commonwealth law that covers the field and achieves the policy aims of criminalising acts such as intentional acquisition, but does not in the process also criminalise acts such as accidental or unintentional acquisition and unknowing possession.

Finally, we ask the committee to carefully scrutinise any proposed new measures for combating crime, to ensure that they are consistent with international human rights instruments and that they would not, if implemented, undermine the long established balance in Australian telecommunications interception law between individuals' right to privacy and legitimate law enforcement needs. That concludes my initial remarks.

CHAIR—Thanks very much. You have provided us with the other side of the coin. We have heard about the difficulties relating to access to records and what we should do, and we have not been thinking a whole lot on that side. From our point of view, and on behalf of the community, we are looking at, firstly, the problem of access to the Internet by hard-core paedophiles and the way they are able to use sites to transmit pornographic child sex imagery; secondly, the problem of access to pornographic sites by minors; and thirdly, the problem of grooming in chat rooms. It is obviously a question of balancing civil liberties and preventing paedophiles gaining access to a new medium to exchange pornographic material with one another and to be able to groom young people, which we have had evidence of in London, for example. How do we balance that out? I am sure that you would be concerned about that as much as we are. Do you have any initial comments?

Ms Graham—No. We certainly have great concern about use of the Internet for that kind of activity. Really what we want to try to emphasise is the need to make sure that any recommendations and proposals are achieving the principal objective without vast abuse of privacy rights. We recognise that at times there is a need for people who may be innocent to be investigated. All of these things, obviously, may have to occur to prevent crime, but their extent has to be limited. It has to be done when there is a serious suspicion of a serious crime, not just loosely, and we have to be certain, for example, that when people have been investigated and found not to have been involved in anything the information that has been collected and stored about them gets deleted in accordance with standard international privacy principles. We are not saying that law enforcement should not be able to investigate these types of crimes, but there needs to be balance and consideration as to how we can minimise infringement of privacy.

CHAIR—In terms of the discussion that we had as recently as this morning, given the hundreds of thousands of emails and transmissions on the Internet, to be able to identify certain ones is difficult. In chat rooms alone trying to sort those out is difficult. On the other hand, how you sort out which ones are serious offenders is the problem. How do you separate out, for example, pornographic spam versus the hard-core senders? Ideas that you have to assist the committee with this would be welcome. I am sure all of us would agree that we do not necessarily want Big Brother coming along and taking hold of our ability to communicate with

one another. On the other hand, we are looking at the evidence we have been provided with—and we have been through the Australian High Tech Crime Centre and ASIC just this morning. One of the previous commissioners of the National Crime Authority said that we need greater handlers, that Internet service providers need to be registered and that we need to be able to follow through who has sent emails and transmissions et cetera.

Ms Graham—I am probably at a slight disadvantage because unfortunately none of the transcripts from the hearings and so forth from last week appeared to be on the parliamentary website over the weekend, so unfortunately I have not been able to hear what they have been saying.

CHAIR—It can take a while.

Ms Graham—It is usually easier to respond to these kinds of calls for greater powers when it is clear what there is a lack of. We need to be clear what agencies say they cannot do in order to be able to respond to whether that is legitimate or whether there are other ways.

CHAIR—As I understand it—and the committee may want to help in painting the picture—if you get somebody who consistently goes to an Internet cafe, and is involved in grooming a 12- or 13-year-old girl and that eventually leads to a sexual assault of a minor, trying to track that through is virtually impossible. The problem is you can get a go on the Net without providing identification and there is no real way of checking back. That is why they are saying that ISPs should provide full details and that in order to gain access to the Internet you should need proper identification et cetera. It is not only an issue of child pornography, it is also a question of credit card and banking fraud et cetera.

Ms Graham—My immediate reaction to that kind of instance is to once again say that, if there is an issue with anonymous use in places like Internet cafes, then there may well be the need for better identification in that regard. That does not mean that the privacy of people who have already identified themselves to their ISP—by giving them their credit card number, giving them their home address and everything else—should have to be invaded further as well, just so that we can track what anonymous people are doing in Internet cafes.

CHAIR—What about those people who are providing bogus names to ISP providers and using false credit cards and whatever?

Ms Graham—Sorry, I was meaning that a vast majority of Internet users do provide their real names to their ISPs. I was looking at it from the point of view that my understanding is that the majority of Internet users have already identified themselves quite genuinely. There may well be cases where people are providing false names, and you would expect that criminals would do that. So there certainly may be a situation where there needs to be a better means of identification, but basically we would want to see what exactly the proposal was and what the conditions were with regard to the security of that information—who it could be provided to and under what circumstances.

We are very concerned about the Telecommunications Act at the moment because it leaves it in the hands of Internet service providers to decide whether they think it is reasonable to give personal information about their customers' activities to government agencies. There is a

particular clause that we have mentioned in our written submission that does not require a police force or a civil penalty agency to even put in a written request for personal information about a person. It is left to the ISP staff to make a decision as to whether they think it is reasonably necessary to give that information to the police officer. How many people in ISP offices are really going to be prepared to say to a police officer, 'I'm not sure that there is sufficient justification to give this information out. Come back to me with a certified request'? Those are the kinds of concerns that we have. Whilst many law enforcement agencies are completely legitimate and only asking about people that they really suspect are committing crimes, at the moment there is too much room for abuse of access to personal information.

CHAIR—What kind of abuse would you see?

Ms Graham—The police and other civil penalties agencies going on fishing trips with minor suspicions that people might be involved in this or that. They might think, 'Because this person communicated by email with that person then maybe they are involved in criminal activity with that other person. So we'll just go to the ISP and we'll get information about everything they've done.'

CHAIR—Isn't that likely, though?

Ms Graham—No, it is not likely. If you have been sent pornographic spam, for example, there will be a record that you and the spammer have been in contact, even though you never asked for the email.

CHAIR—But you are not really talking about seeing who else somebody who receives spam has been in contact with. Aren't you really talking about seeing whether somebody who they suspect is a child sex offender is in contact with others, to see if there is a trail of other paedophiles who may be in contact and downloading pornographic images?

Ms Graham—We would hope that that would be what they are looking into. But what I am saying is that the way the laws are currently written gives agencies the ability to access a much broader range of information than that. So we believe that the kinds of things that we understand agencies are asking for, like mandatory retention of all Internet activity, would give far too many agencies—for far too many minor crimes—the ability to get complete details of everything a person had been doing, for however long. And we are saying that, if that is going to happen, the laws need to be tightened to have more control over who can access that, through some form of parliamentary or judicial oversight. We are not saying that law enforcement agencies can never have access to information. We are saying that there are not enough controls and there are too many loopholes in the existing laws. So if there are going to be demands or requirements put in place for Internet service providers to log information then there also have to be, in our view, changes to the law to put more controls in place as to how this information can be used.

CHAIR—Like a cyber-ombudsman?

Ms Graham—Perhaps so. What I am saying is that three-quarters of a million disclosures of information are made every year about calling numbers and general information about telecommunications users, without any recording of the circumstances as to why they were released—there is basically no oversight of that at all. We are saying that, while it is all very well

that under these particular sections of the Telecommunications Act they can get access to calling and called numbers, the concern is that those exact same laws can be used to access details of every single webpage a person visits, every single email they send or receive—and the list goes on and on. It is the same as having a camera over your shoulder the whole time when you have been going to a library, going into a shop and walking down the street. It is the same as it would be if your life had been recorded and then some civil agency got a suspicion that you might be involved in something. The concern is that they are going to be permitted to have access to this vast range of communications data. So what we want to stress is that there needs to be controls on and oversights of this.

CHAIR—Do you agree that, under certain circumstances, this is a totally valid thing to do?

Ms Graham—It depends on what 'this' is. We do not believe that storing everything that everybody does is valid. For example, in the UK at the moment they are basically deciding that that is not valid either. Although the UK decided that they were going to do that, there was so much public outcry and then investigation into the EU data privacy directives that the government basically had to back down on its proposal. They now have a consultation paper out to review this whole matter, because they decided that it was not acceptable to record everything that everybody does just in case it might be useful down the track. You have to remember that people who are using the Internet are also real people out on the street. There is a real question as to how much use will be made of some of this data in the first place and whether people would not be caught anyway. Perhaps I could give an example: if someone is suspected of being involved in illegal activity, ISPs are already in a position to make sure that every time that person logs in they get connected to the same IP address, and the ISP can then record every single thing that individual does for the next three months.

CHAIR—Do you see that in the case of someone who is suspected of being a serious child sex offender it would be of interest to find out who he or she is in contact with, what sites they are accessing and what chat rooms they are going into et cetera?

Ms Graham—That is what I meant by what I just said. If such a person is suspected, we believe there are already laws that enable the police to require the ISP to monitor that particular person's activity. It can already be done under the Telecommunications Act; it is being done by police forces regularly, I am told. ISPs receive requests to ensure that a particular individual's activities are monitored. They make sure that when the person logs in they get the same IP address—that is, a data address that shows how you are connected to the Internet—and, from that, they can record everything that that individual does. If there is a valid warrant to monitor a particular user then, as I say, they can do it now, so I keep having difficulty understanding what it is they are saying they cannot do.

Senator HUTCHINS—Are you saying that they are doing it now without a warrant?

Ms Graham—I am under the impression from what I have been told by ISPs that at the moment, if a police officer goes to an ISP and says that they want to know what a particular person is doing, the ISPs do it. I believe it is being done without a warrant, but some ISPs might be insisting on a warrant; ISPs basically have a level of choice. Because this is a particular issue where it is real-time monitoring, some ISPs may feel they should not do it without getting a search warrant. I understand that they are certainly doing it without an interception warrant

under the Telecommunications (Interception) Act—I understand the interception act is not being involved at all. They are doing it under the Telecommunications Act. So, in effect, from what I have been told—and if I am wrong, then I have been lied to—ISPs do connect a particular individual to one IP address so that they can track every webpage and every email easily. They could do it anyway, but the purpose of making sure the person always connects to the same IP address is just to make it much easier for them to go through all their logs and data match that number to quickly find out what a particular person has been doing. As I say, I am being told that they are doing that now without a warrant.

Senator HUTCHINS—This is an inquiry into crime, and in your summary you talked about an impetuous desire to counter crime. Why shouldn't police be able to do that? Do you have any evidence that they are abusing their access to these ISPs for any other reason? We have had evidence about child pornography and earlier we heard about trillions of dollars being stolen each year in credit card scam.

Ms Graham—Trillions?

Senator HUTCHINS—That was one report.

Ms Graham—It was supposed to be $3 trillion in the last law enforcement implications of technology inquiry and no-one could ever identify what—

Senator HUTCHINS—It does not matter whether or not it is $3 trillion. If it is $2 billion, it is $2 billion too much.

Ms Graham—Yes.

Senator HUTCHINS—This is an inquiry into crime, so I would like you to respond, Ms Graham.

Ms Graham—I believe the police need the ability to intercept and monitor certain types of activities. EFA believes that. As I said, we support the need to combat crime, but we believe there needs to be oversight of police powers. We think whether a particular police officer is or is not corrupt or is or is not generally doing the right thing is beside the point. We believe people have a fundamental human right to not have undue, unnecessary, unauthorised access to their personal communications.

CHAIR—It is still a key question. Do you have any evidence that the information gathered is used inappropriately?

Ms Graham—It is minor, but I remember one particular thing that just makes you wonder. A few years ago on a public discussion list the wife of a police officer got in and proceeded to try to claim that a particular person was using a false name, because her husband had looked up the motor vehicles database and found that no such person in Brisbane had a drivers licence. So the person, who was just having a general chat in this discussion forum, was being accused of lying. Eventually the police officer joined in the discussion and said, 'I am sorry, I realise I should not have done that.' It was only minor, but these are the kinds of things that you see happening when you are around the Internet, and you wonder what else is happening that you do not know about.

So we say that the law therefore needs to put controls over who can access information and make sure there is judicial oversight over whether there is a real need to have access to the information.

Senator HUTCHINS—On page 6 of your submission you say:

Although there might be questions about some particular cases, the fact that a complaint can result in a police raid of an innocent and well-intentioned individual's home is cause for grave concern.

Do you know of any incident where this has occurred?

Ms Graham—Where people have been prosecuted?

Senator HUTCHINS—No, you say 'a police raid'. Have there been any incidents where, in your opinion, access to these ISPs has been abused by the police?

Ms Graham—I am not aware of an instance in relation to the police, because I do not have—and, as far as I am aware, no-one else on the EFA board has—access to information as to what kinds of requests the ISPs are receiving from police. We do not have access to that. We have had ISPs tell us about the ways that they provide information to police, but no-one will tell us what is basically confidential information. I cannot comment, I am sorry, on whether there are any instances.

Senator HUTCHINS—It might not have happened.

Ms Graham—Exactly, it might not have happened, but the way the law is written at the moment enables it to happen, and so we are saying that before any more access or more retention occurs that needs to be fixed.

Mr SERCOMBE—But Ms Graham, when you have had discussions with ISPs about this, when these issues have been raised with you, have they been raised in a context where the people associated with the ISPs have been expressing a concern about the approaches they have been receiving from the police?

Ms Graham—The discussions I have had personally with a couple of ISPs have been when I have phoned them to ask them if they would tell me under what circumstances people's activities were being traced in terms of what I was talking about with those IP addresses. I had heard rumours about that, but I honestly cannot remember—it is 12 months ago now—where the rumours originated. When I say 'rumour', I cannot remember who told me. I phoned a couple of ISPs that I knew, one of whom is a law enforcement liaison for one particular ISP, and he was willing to tell me about this process of IP addresses.

Mr SERCOMBE—Given that it is a public inquiry, are you prepared to tell us which particular ISPs you had those discussions with?

Ms Graham—I am sorry; not in a public inquiry—not in a public transcript.

Mr SERCOMBE—Would you provide it in camera to us?

Ms Graham—Yes; only because I do not think it is appropriate for me to name which particular ISPs have been providing me with information.

Mr SERCOMBE—But you are making very important points and it would be useful for the committee.

Ms Graham—I am quite happy to give them to you separately, provided they are not going to be named in *Hansard*. I believe that they are people who would be quite happy to talk with you.

Mr SERCOMBE—Thank you. Could you tell us a little more about EFA by way of background, Ms Graham? You describe yourself as a non-profit national organisation representing Internet users. Could you paint us a bit of a picture as to this body, who it represents, and perhaps how it raises funds?

Ms Graham—I realised that was going to be the question. We are completely funded by membership subscriptions and donations from people with an altruistic interest in civil liberties. I am aware that a number of our detractors claim that we are funded by the pornography industry. At least one senator has implied that on numerous occasions, and it is not correct.

CHAIR—Could we ask you for the breakdown of your membership fees? Having once in my past life run a membership organisation, it was clear who called the shots in terms of what the percentage was. What do they represent? Do pornography suppliers provide funds to your organisation?

Ms Graham—Not to my knowledge. We have a membership structure whereby people can join on an annual basis for $20. We are largely a voluntary organisation. I am the only person who is actually remunerated for services to the organisation. Everybody else—the board—is a volunteer. We invite members of the public to join EFA if they wish.

CHAIR—How many members do you have?

Ms Graham—I am sorry, but we do not publicise that information.

CHAIR—When I was with the Tourism Council, for example, we published the list of our members so that people would have a clear idea of who were our providers. You are making the claim that pornography suppliers are not part of your membership. Don't you think you are asking us to take that at face value, if you will not provide a copy?

Ms Graham—Yes, I am.

CHAIR—Are you prepared to provide, in camera, your membership list?

Ms Graham—Absolutely not. Our members are advised that they have the same privacy rights as anybody else in this country. Under no circumstances do we provide lists of members to anybody.

CHAIR—But if you are a lobbying organisation, it is normal that governments know who they are dealing with.

Ms Graham—Yes, and we are a registered, incorporated association. We have been in existence since 1994. The names of the board members of EFA are publicly disclosed. We put all of our policies and information about our submissions on our web site. There is nothing secret about EFA, except that our members are entitled to their privacy.

CHAIR—Do you have different levels of membership in that some pay more than others?

Ms Graham—Not really, but I will explain what I mean by 'not really'. Our annual membership fee is $20. You pay $20 to join as an individual member. Or, if you prefer, you can pay EFA $100 for life membership.

CHAIR—But do you have particular sponsors above that?

Ms Graham—Yes, we have people who provide donations.

CHAIR—And organisations?

Ms Graham—Yes. Some are individuals. It is not necessarily organisations. Certainly none of the larger sponsors are involved in anything to do with pornography. I really wish to stress that, because EFA finds it quite offensive that we keep getting these suggestions that we are funded by the pornography industry. We are not and we never have been.

CHAIR—I am not suggesting you are.

Ms Graham—We were established in 1994 because of concerns. I realise that you are not suggesting that, but almost every time I appear before a Senate or a House committee, this issue comes up. Sometimes it has come up—not in my presence—even in the Senate, where it has been implied that I personally, or EFA, work for the pornography industry. I find it offensive because it is so blatantly untrue. I object to it.

Mr SERCOMBE—No-one here is suggesting that, Ms Graham.

Ms Graham—I am sorry, but every time we are asked about membership and where we get our funding from it is something to do with the context of pornography. I just want to make it clear that that is not the case.

Mr SERCOMBE—I assure you that was not my motivation in raising the matter. I raised the matter because I actually think some of the points you make are important points that need to be put into the balance. I was simply wanting elucidation on where you were coming from, because the description in the submission does not really take us very far.

Ms Graham—I can give you a little bit more information—we can get off the other topic and get back on to this.

Mr SERCOMBE—Perhaps we can deal with that in camera.

Ms Graham—Yes. We have got a lot of people that are involved in IT. We have a lot of supporters that do not actually bother to pay $20 but they email us offering help and information.

It is a bit like a political party—a lot of people do not actually join, but they support it. We have a lot of people who are very much involved in IT and technology. But we do not actually know what the particular interests of a lot of our members are. They are just people willing to pay us $20 because they like what we have been saying and doing for the last seven or eight years or something. To be honest with you, I do not know who half the members are, apart from them telling us which particular aspects they are interested in. On our membership form it says,' Please mark what you are interested in, if you want to.' There is censorship, privacy, cryptography, intellectual property and Net regulation generally, and most people tick all of them.

Mr SERCOMBE—Moving on to an issue of substance in your submission, you talk about the prospect of someone who is unknowingly in possession of pornographic material facing the possibility of criminal action against them. In appendix 1 you have produced extracts from various state and territory laws. I take your point in relation to the ways in which some of these items in the various crimes acts are specified, but it would be my understanding that it would be almost inconceivable that a DPP would proceed against someone—let alone a court convict them—for an offence relating to child pornography if, in fact, that person was unknowingly in possession of it. Please correct me if I am wrong, based upon any experience or knowledge that you might have. Some of the legislation makes the 'knowingly' component of the offence part of the definition, and I think that is important and good. It is a pity that some of the other states do not do that. I am not a lawyer, but it is a fairly fundamental part of my understanding of criminal law that you are not going to get a conviction for a criminal offence unless intent is demonstrated, or—using that Latin phrase, mens rea—a guilty mind. In the absence of intent, I would have thought that a DPP in any jurisdiction is highly unlikely to proceed and, even if they did, they would not get a conviction. Are you aware of people who have been convicted under these circumstances?

Ms Graham—Not convicted, but there are people who have spent 18 months fighting a conviction in court. There is one case that I am personally familiar with—I think it started in 1996, but forgive me if that is not exactly the right year, in Queensland. It was claimed that an ISP had found material involving child pornography in temporary directories on the ISPs computer system. The ISP claimed that there was information within their temporary directories that suggested that a particular 21-year-old man had downloaded this material. He claimed that he had never seen such material on his computer et cetera. This went through the court in Queensland for 18 months, and in the end the judge instructed the jury to find him not guilty on the grounds that the police did not have sufficient evidence. That is a very brief summary. It cost this person $17,000 to fight this case.

Mr SERCOMBE—As unfortunate as those circumstances are, I think your point supports my point: a person is not going to be convicted. In fact in my view it is unlikely to proceed as far as that.

Ms Graham—One would certainly hope not. But there are a lot of courts that still do not really understand the technology. We would have some concerns about the level of technological understanding of some courts, DPPs and so forth. I would not be willing to go so far as to say that they would never be convicted but our point is not just the issue of whether a person would be convicted. People who are accused of being in possession of child pornography get splashed all over the newspapers. In this particular case in Queensland, with this young man and his

family, there was absolutely no proof that any of them had ever been involved in anything illegal. But everything was splashed across the newspapers et cetera. It would never have happened if the laws did not disregard to such an extent intent and knowledge. That is our concern: if people are not going to be convicted anyway if they did not know and did not intend, why can't the law say that?

Mr SERCOMBE—If I were a police commissioner, I would be very angry about the officers wasting resources and proceeding with such a case.

Ms Graham—Fine, so let us fix the laws so that they say, 'You have to have knowledge and intent,' and then everybody will be happy, including the police officers whose staff waste the time of the courts. There was another case in about 1998, where it was claimed—and I have no personal knowledge of the background, but this is what was reported in the newspaper—that a person in Canberra had received some illegal material that had been sent in a file during an Internet relay chat session. For reasons that I do not know he apparently did not immediately report it to the police, but he did subsequently report it to his employer, which was a government department. The government department reported it to the police, which is fair enough. He was convicted. My understanding from the newspaper reports is that he did not intend to receive that material in the first place. But it appears—from the limited information in the newspaper reports—that because he failed to report it immediately it was considered that he had intentionally kept it for some period of time. I have no real comment on that aspect of it, but the fact is that that person had not intended to receive that material in the first place.

The issue is: if you have received information like that and then go and report it to the police, you can be prosecuted immediately for being in possession of it. So you cannot report it, because you can -incriminate yourself. This could be exactly this guy's situation. He did not report it. He claimed that he had become so concerned about the fact that this information was available that he decided he would report it. And then he still got prosecuted and convicted. I have no idea about this particular person.

Mr SERCOMBE—What was he actually convicted of?

Ms Graham—Possession of child pornography obtained over the Internet. It was in about 1997. I think the case probably was not decided until 1998.

Mr SERCOMBE—Mr Chair, noting the time, could I move that we go in camera?

CHAIR—Senator Greig has not had a chance to ask questions yet—not that it is obligatory, Senator Greig.

Senator GREIG—I am captivated by the discussion. I have more of an observation than a question really. It seems to me that what you are saying—and I am paraphrasing—is that you have no objection to appropriate police powers for the investigation of possible prosecution for crime within the Internet world, provided that there is some kind of oversight and regulation. I guess that is the issue that we are struggling with here.

Ms Graham—Yes.

Senator GREIG—All too often the debate comes down to child pornography. I am not trying to diminish how horrendous that is, but there are so many other issues out there that I think can and should be addressed as well. I would make the observation too that, given that there have now been police royal commissions into corruption in three if not four states, time and again we have found that in many cases police cannot be trusted and have abused powers, often for political reasons. One of my concerns is where you have a situation where police may check emails without warrant from Internet servers for political information—who is emailing whom and for what reason. So I have no argument with you there. I have one question with respect to your submission. You argued in part that there were flaws in existing laws that prevented users from reporting criminal activity. I am not quite sure that I follow that argument. Can you demonstrate for my benefit?

Ms Graham—What I mean is the flaw that means that you can be convicted of possessing child pornography, for example, when you report it, because the law in some states does not say that you can only be convicted if you knew it was there and intended to receive it, or similar to that. Because it does not say that, there is a situation where you cannot report that. In my opinion a sensible person would not report the fact that they had received child pornography in spam to the police, because they would risk spending the next 18 months fighting a court case. I find that really concerning. If I received child pornography in spam, I would want to be able to report it to the police so that somebody—the police—could try to find this person and do something about it. However, I can tell you quite absolutely that I would not report it to the police, because I do not want my name splashed across the newspaper as a child pornographer, and I do not want to spend $20,000 fighting a case in court to prove that I did not ask for this material and they should not convict me. I do not see how I could possibly be expected to report having received child pornography in spam to a police officer, knowing that there is absolutely nothing to stop them from then deciding to prosecute me. Seriously, how many of you would report it?

CHAIR—It is the downloading and storing that is meant to be an offence; just viewing or receiving it is not the offence, as we understand.

Ms Graham—There are very few states that have laws that talk about using a computer system to receive something. The Western Australian law is slightly more sensible than some of the others in this narrow area. It talks about intentionally—that is one of the laws that has words such as ‘intentional’ or ‘knowingly’ using a computer service to obtain possession. Western Australia is probably the only one that talks about actually using a computer service to obtain possession. I am pretty sure that all, or close to all, of the others only talk about the mere fact of possession. That means it is on your disk. It makes no difference whether you got it from somewhere on a floppy disk and then put it on your hard drive, and that is possession, or whether it came across the Internet. The fact is that, because it is on your computer disk, you are in possession of it. The other aspect, which we also raised, is that if you accidentally clicked on a webpage and it turned out to have stuff on there that you never expected, that is in your web cache. Even when the web cache automatically gets cleared from your computer, the file is still on the disk. Most individuals have no idea how to delete material. They think that clicking ‘delete’ on a Windows system deletes the file. It does not delete the file; the file is still on the hard drive. Under all these laws, even if you actually clicked ‘delete’ when you discovered you had got something you did not want, if your computer were ever seized and the police searched it, with their software tools they would find the deleted files and you could be prosecuted. Even

though you have taken affirmative steps to delete the material, you can be prosecuted. You might not get convicted, but it is still a fact that you can be prosecuted.

Evidence was then taken in camera, but later resumed in public—

[3.22 p.m.]

HENLEY, Mr Graham Donald, Director, PricewaterhouseCoopers

POBIHUN, Mr Scott, Manager, PricewaterhouseCoopers

CHAIR—I reconvene this public meeting of the parliamentary Joint Committee on the Australian Crime Commission. The committee is examining recent trends in practices and methods of cybercrime, with particular reference to, firstly, child pornography and associated paedophile activity; secondly, banking, including credit card fraud and money laundering; and, thirdly, threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role that the newly established Australian Crime Commission might play in combating this crime.

I welcome the next witnesses, Mr Henley and Mr Pobihun of PricewaterhouseCoopers. The committee prefers all evidence to be given in public, although from time to time we do consider requests for evidence to be given in camera. If you wish to do so, please ask the committee, which will examine your request. I invite you to make your opening statement, and we will follow that with questions.

Mr Henley—Perhaps it is best if I give the committee some background as to what our organisation does in this field.

CHAIR—That would be great.

Mr Henley—PricewaterhouseCoopers has a fraud investigations team. We have approximately 43 people Australia-wide, mostly based on the east coast of Australia, and we do a wide variety of fraud investigations. A lot of our work comes internally from PricewaterhouseCoopers clients. A lot of investigations, as you can imagine, come out of our audit capacity or existing audit relationship clients, but at least 40 per cent of our work comes from clients for which we do not have another, existing relationship. Our investigation team employs a wide variety of people. There are quite a number of ex law enforcement officers there. I look after what we call our Computer Forensics and Electronic Investigations team. There are currently nine people on my team. Our team has computer forensics practitioners in Sydney, Melbourne, Brisbane and Canberra. We also have people in Hong Kong, Jakarta and New Zealand; we operate within the Asia-Pacific region. We have strong computer forensics and electronic investigations capacities worldwide. There are about 95 full-time staff in the US and, again, staff in the UK, Europe, and South Africa.

In our role, we are really a reactive team; we come in and investigate after the event. We have other areas within PricewaterhouseCoopers that look after security reviews, intrusion testing et cetera, but we really are a reactionary investigations team for the majority of the work that we deal with. Probably 70 per cent of the computer forensics and investigations work that we do would come from the private sector. That could be broken down into some broad areas. We do quite a bit of work on litigation and administrations that PricewaterhouseCoopers as a firm are involved in. Usually these are cases where it is alleged that directors et cetera have stripped

assets out of a company that has gone into administration or liquidation. A lot of work recently has related to the theft of confidential commercial information. This usually involves employees going from one business to the next. Some of our big clients are involved in the software industry, so we do a lot of work with the theft of intellectual property and people distributing intellectual property online. Then there is a range of work that we do that can be basically referred to as employment law, which is really the misuse of computer systems: surfing of the Internet for pornography—obviously this involves child pornography in some cases—running another business on your employer's computer, and that whole range of things that employees get up to that perhaps they should not. Then we do our mainstream fraud investigations. Computer forensics and electronic investigations are always a component in any traditional fraud investigation that we do.

Another 30 per cent of our work is for government agencies. Really that can be broken down into the regulatory work that we do with ASIC—that is a large percentage; we assist a lot with search warrants for ASIC—and the work we do directly for law enforcement. Most of our work comes out of the New South Wales Police. When their electronic investigations team or their special technical investigations branch, as they call it, is overloaded with work they push the work out to the private sector. We often pick up cases involving child pornography or really any type of fraud from them. In fact, just yesterday we were referred a murder investigation and were asked to examine computers on behalf of the New South Wales Police.

In our submission we have included some statistics. PricewaterhouseCoopers has done a global economic crime survey, and we have included that for your perusal. There are some comments there about cybercrime. I guess the principal statistic is that in our survey 38 per cent of people perceived cybercrime as a significant threat in the next five years. We see that the main issues of cybercrime that would be of relevance to the inquiry are the ones relating to jurisdiction—being able to investigate matters across jurisdictions all around the world. My background personally is that I spent 11 years in the Federal Police, with the last five years in the computer crime unit in Sydney. I left there in 1997 and moved out to the private sector. So I have a picture of life inside law enforcement and outside law enforcement.

We are also starting to see a trend with the Internet being used to move moneys around with Internet currencies. The legislation being able to keep pace is obviously a challenge. In the cases we are involved in, we have seen an increase in the use of protection tools and disk-wiping software to remove evidence and an increase in the use of Internet tools to anonymise the activities of suspects, making the investigations more difficult. We are often the middleman, if you like. The corporate sector may come to an organisation like us to conduct investigations, and we may pass the matter on to proceed through the civil courts if, working with their lawyers, they decide that that is the course they wish to take. We may also even refer a full brief of evidence to law enforcement. Again, in some of those cases we actually go out with law enforcement and assist in the execution of search warrants et cetera.

In our investigation of cybercrime, one of the difficult factors that we in the private sector have is that it is not possible for us to get direct information from Internet service providers. We either refer the matters to the police or, if they are not law enforcement type matters, try and pursue the information from Internet service providers through the civil courts. That can pose problems for us because really the civil courts are inexperienced in dealing with these matters. In many cases in the civil arena you must have a respondent to the proceedings before you can set

the proceedings in motion. We have got information from Internet service providers by way of preliminary discovery. That, again, can cause its own problems, because it may push the matter down a civil course where, perhaps, it might turn out after the investigation has progressed that it is more suited to being a criminal matter.

Similarly, we have no ability to get information from a telco. Obviously in cybercrime matters the ability to get effective information out of Internet service providers and telcos very quickly is essential in trying to identify the source of the attack or the source of the suspect of any investigation.

We have a lot of dealings in the corporate sector with people who are the IT representatives of companies, so we see how companies try to assess investigations and incidents that happen within their organisations—then they come to us, in many cases, for advice. We see that there is not a lot of clarification about the things that people can lawfully do within their organisation to try and detect crime. For example, we know that, to try and identify the crime, a lot of people place keystroke loggers and those sorts of tools on computers that they think suspicious activity might be happening on, yet there has been little consideration given to things such as the Telecommunications (Interception) Act and whether or not these tools can be appropriately used in relation to those acts.

The final point we would like to raise is that we see a need for some consistent training and standards within Australia to raise the level of cybercrime investigation. We would like that open to both law enforcement and the private sector, as we feel that we are an important component that can assist the law enforcement agencies in the investigation.

CHAIR—Thanks very much, Mr Henley; that was comprehensive. My colleagues might want to lead off first, but while they are thinking about their questions I have just a few. As you outlined, you have identified four techniques which promote cybercrime—anonymous Internet activity, social engineering deception, system exploits and data-scrubbing software. I wonder whether you can elaborate on the term 'social engineering' and its significance for cybercrime. Also, what can we do to address each of those in turn—or can we?

Mr Henley—That is the difficult thing, I guess. Social engineering is the tool of trade of any person wanting to commit fraud. Social engineering is getting a person's confidence so that they may tell you information that you should not rightfully have. Probably the best way to explain it is to go back to a case I did in law enforcement. A person built a device out of parts of a water heater, and he would take that device down to a public telephone box and use it to make free calls. He would get on the phone, ring random people in the US, pretend to be an AT and T operator and say, 'Did you receive a call from Wyoming on Tuesday night for 20 minutes?' They would say no, and he would say, 'I'm from AT and T. We have a cross-billing error in our system here; we need to rectify the billing error. Can you please provide me with your calling card information.' He was using social engineering to collect their calling card information. That would allow him to use the calling card to make free calls, but he would also take that number back to the Internet and sell that calling card number to other people around the world.

CHAIR—They used to call them con merchants.

Mr Henley—It is very much the same principle.

CHAIR—'Social engineering' kind of has a better ring to it though, hasn't it?

Mr Henley—Yes.

Senator GREIG—When you sell a calling card number like that over the Internet, how do you get paid for it?

Mr Henley—He was using cash sent through the post. A lot of the other types of systems are sent by courier or use cash on delivery. There are also now these currencies on the Internet called e-cash, e-gold or Evocash, in which you can turn your currencies into an Internet dollar, if you like, and redeem them that way. So there are many ways.

Senator GREIG—I was just thinking, though, that it would strike most people as a con within itself if they were told that if they sent the cash they would be sent the number, wouldn't it?

Mr Henley—Yes, but he was definitely supplying the numbers. He was making a considerable amount of money out of this particular activity. Social engineering really represents what a lot of fraudsters, if you want to call them that, do. They put themselves in a position of power. You may rifle round in a rubbish bin, find some contact information for an organisation, ring them up and say, 'My name is such and such. I have a problem logging on to my computer. I am getting these particular errors.' You are after some sort of relationship with the IT department. The help desk could allow you information that would be able to penetrate their network. It is a fairly straightforward tool.

As an investigator, when you speak to people, you are never overtly nasty. Really you are socially engineering every time you are seeking information from somebody. That is the way investigators work. I think it is the way that the world works. It is certainly nothing new; it is very much the con of old.

Mr Pobihun—You could also consider, with online chat systems like Internet relay chat or Yahoo, that if you are in a chat room speaking about a certain stock you could be trying to influence them to change their commercial activities, therefore modifying the value of the shares as well. So you could be modifying the stock market through social engineering online.

Mr Henley—Another example that you would be interested in is to do with people involved in child pornography activity. If they are on a chat line pretending to be a 13-year-old female in order to attract similar people and have similar conversations then that is a very pertinent example of social engineering.

CHAIR—When you go into companies and find evidence of child pornography, what do you do about it?

Mr Henley—We are in a bit of a difficult situation in the private sector because we work within New South Wales, and the New South Wales Crime Act says that if you possess child pornography you are committing an offence. We are often engaged by the New South Wales Police to investigate matters of child pornography. We take a forensic image of the computer system, we examine the computer system and we find child pornography. In these cases, we

immediately notify the police as such and we seek instructions from the police to continue our investigation or continue our possession of the material. We seek that in writing from them before we proceed. If that does not come, we immediately hand over all the material that we have straight to the law enforcement agency.

CHAIR—What happens with private companies?

Mr Henley—If we are engaged, as we were recently, by a private company through their lawyer and we find child pornography, we immediately advise the company and their lawyers that we found child pornography and that their obligation is to report it to the police. We may seek our own internal legal advice from our in-house counsel about whether PricewaterhouseCoopers, as an organisation, should directly go to the police. We rely on our in-house counsel's advice in each case as to what is appropriate.

Senator HUTCHINS—Is each case each state?

Mr Henley—No, in each individual investigation.

CHAIR—When is it not appropriate for you to report it to the police?

Mr Henley—I cannot think of a case we have not reported to the police. But we make sure that we get advice that we can hold up and say, 'This is what we were instructed to do.' Most clients, I would say, have an initial hesitancy to have the police involved. In many cases that come across our doorstep, the clients have an absolute objection to going anywhere near law enforcement. But in cases where child pornography is involved, all the cases that come through us—in my knowledge—are reported to the police, usually on our recommendation, as the legislation requires.

CHAIR—You were there when Electronic Frontiers gave their evidence to us today and you heard their views in terms of access et cetera. I heard you talking about the problems that you have in terms of getting access—you need to go to the courts et cetera. Does that happen often?

Mr Henley—Yes, it does. With most Internet investigations we are involved in, you need access to ISP records or telco records to progress the Internet investigation past a certain point.

CHAIR—What normally happens when you request them?

Mr Henley—If we come across an instance where we need them, because of my ex law enforcement association—only because of our in-house knowledge—we directly ring the law enforcement liaison officer for the larger ISPs and say to them: 'We need you to preserve the records now. We don't know whether this will go to law enforcement, but it may go to the civil courts. We may come back with a subpoena.' But, generally speaking, if we do not go to law enforcement, a subpoena may be six months down the track, which in terms of cybercrime is infinity really.

Mr SERCOMBE—Do ISPs invariably comply with that request?

Mr Henley—Usually.

Mr SERCOMBE—But not always?

Mr Henley—I have had instances where the ISPs are reluctant to even talk to a private sector organisation.

Mr SERCOMBE—You cannot go around and have a friendly chat with them?

Mr Henley—No. We ring them and we explain the situation. If they preserve the records for us, well and good; if they do not, there is not much we can do.

Mr SERCOMBE—There is no legal obligation for them to do so?

Mr Henley—I do not believe there is any legal obligation for them to hold records. I do not think there is a legal obligation for them to keep records in the first place.

CHAIR—Should there be?

Mr Henley—Certainly as an investigator I would like to see it.

CHAIR—You have heard the other side of the argument this afternoon. What do you think of the arguments in terms of civil liberties?

Mr Pobihun—Perhaps there is a physical limit that needs to be considered, particularly with the larger ISPs where the issue will be how much information they can store.

CHAIR—And for how long. What do you think is feasible?

Mr Pobihun—As Graham has just pointed out, six months in a cyberinvestigation is a huge period of time. Within six months, there will not be any records that we can come back to. It is quite hard to really consider. Obviously there are large ISPs, which you are well aware of, but there are also the smaller ISPs. It will be a lot easier for them to record a week's worth of information than the larger ones.

CHAIR—If you had your way, what would you like to see?

Mr Henley—We have cases that are quite common, where people use ISPs to connect to their web browser and to surf the Internet. In a case where they are surfing child pornography sites and they are trying to identify them, if that connection activity is controlled by the Internet proxy server—a machine that will basically store logs of all the users connected to that ISP over time—generally you would get 24 hours for the larger ISPs, purely because of the volume of records that that ISP has to keep. The old argument for ISPs was that it was too expensive and too time-consuming to store information, but these days I do not think you can fly that argument from an ISP's perspective, because storage has dropped dramatically in price. You can get massive amounts of storage quite cheaply, and you can automate a lot of these processes. I would like to see in those instances at least seven days. If you have not come up with the idea that you need information within the seven days, I think you have missed your window of opportunity in any case.

CHAIR—What about tool-stroke interceptors? How effective do you find them?

Mr Henley—Are you referring to the keystroke logging type devices?

CHAIR—Yes.

Mr Henley—They are very effective. A keystroke logger will record every single keystroke, including backspaces, corrections and any key pressed on the keyboard. They can give you a complete picture of what happens on a person's computer. The thing that is confusing about their legality is that, if a person is engaged in communication with somebody on the other side of the world using their computer, technically speaking there are similarities between that and a telephone call. No-one really has any clear indication, as far as I am aware, as to whether they would be breaching the Telecommunications (Interception) Act if one of these 'keystrokers' were used to log an Internet relay chat conversation, for example. Of course, in our legal system these things will one day be tested. I guess we have nothing to go on at this point in time.

CHAIR—We have been looking in the child pornography area at Net Nanny et cetera. Do you find such programs effective?

Mr Henley—Generally speaking, no. The majority of experience I have had is that both young offenders and relatively savvy Internet users have many ways and means of moving around those systems. Perhaps, if you are a family and you control your children's access to the Internet, Net Nanny or a similar product could be your first step, but really if they have any will or power to do so they can sidestep them quite easily.

CHAIR—So parental supervision is the answer?

Mr Henley—It comes back to that.

CHAIR—In talking about standards being established and so on, do you think there should be a voluntary code developed by the private sector—undoubtedly in consultation with PricewaterhouseCoopers—or should it be government imposed? I think I have a clue as to what your answer might be.

Mr Henley—We feel that Australia really has not gone very far down the track of raising the standard for Internet investigations. Certainly the new organisations that have been set up—and the Federal Police now have a big centre here—may address how we raise the standards. I foresee something available to both the private sector and the public sector, but I would like to see, through an academic institution, qualifications that set a standard. There are some tools out there for investigations such as EnCase, which is the commonly used forensic imaging program. Anyone can buy that for about $A5,000. We now have a lot of people coming into the marketplace in this industry who have very limited experience or instruction in using these tools. They conduct forensic examinations; there may be material missed and it still ends up before the court. It is starting to have an impact on the court aspect of the standard of forensic evidence. Obviously that will work itself out over time. Let us hope that the people who are not professional in their investigations fall by the wayside.

At the moment we would like to see some professional standards set within Australia. We believe Australia has a perfect opportunity to become the focus of training in cybercrime investigations in the world. Instead of sending my team off to the US to have them trained, I would like some qualifications here that we could use.

CHAIR—Why do you think we could take that lead?

Mr Henley—From looking at the training that is available. I have done a number of courses in the US. A lot of US companies come to Australia and present courses purely because of the commercial aspect, purely because there are the numbers out here to make money from the sale of the software and the training of the staff. Really, the courses I have been on in the US are not something that Australia cannot provide, and I think we can provide probably a higher qualification, a better standard or certainly a better structured course to put our investigators through. I think it would raise the level and have a positive impact on the amount of fraud that is identified here and the number of cases that are successfully prosecuted.

Mr SERCOMBE—Are there significant job opportunities in the field?

Mr Henley—Yes.

Mr SERCOMBE—You, Mr Henley, come from the AFP. In most circumstances the private sector is likely to be able to pay significantly more for talent than perhaps the police forces. How do we ensure that the law enforcement agencies themselves have an adequate supply of people to do their functions without running the risk of somewhat more attractive approaches being made from the private sector to poach them?

Mr Henley—It has been a problem. Of the team that I employ, nine of us are currently in Australia. There are 15 of us in the Asia Pacific and nine of those are ex law enforcement; nine of those come out of the police computer forensics teams. We sought people with investigations experience who were able to make the transition to the commercial world. There is no doubt that the place we looked was law enforcement, much as I came out of law enforcement myself.

Mr SERCOMBE—Do the policemen working in the high-tech areas have adequate career paths, or is it still seen as a little overspecialised in terms of promotional prospects?

Mr Henley—One of the main reasons why I left in 1997 was that I had no opportunity to be promoted and no opportunity to earn more money. You could devote your life to chasing cybercriminals—put your heart and soul into it—and at the end of the day you were pretty much—

Mr SERCOMBE—You cannot pay the mortgage.

Mr Henley—Yes, that is right.

Mr SERCOMBE—In your view, are things changing in law enforcement?

Mr Henley—I think that they are. The Federal Police have gone through a great restructuring. There are a lot of different remuneration characteristics within the AFP; they are on a composite

wage et cetera. Certainly the salary of a Federal Police officer has considerably increased. They have a new structure now, a cell structure, whereby they have the opportunity to get promotions. My perception of it is that it has increased somewhat. I still do not think that they can match the private sector.

Mr SERCOMBE—Perhaps it is a bit harder to poach now than when you were poached, but it is still not impossible?

Mr Henley—It is not impossible. I think that the other thing is that there was a massive staff increase in private sector fraud investigation teams for a number of years. That has started to plateau now. The major accounting firms have investigation teams. There are quite a number of second-tier firms that have since folded because they cannot bring in the work. So I think that the staff numbers in the private sector have started to flatten. We are not seeing that rapid increase now, and consequently the incidence of people being brought out of law enforcement has reduced naturally because of that.

There are some reasons why you would like to work in law enforcement—do not get me wrong. Some of the cases that the AFP or other cybercrime investigators get to work on are the high-profile cases, which are attractive to certain types of investigators, whereas, in the private sector, you may be more likely to look at directors stealing assets in liquidation, for example. There are pros and cons.

CHAIR—It has been claimed that we have an oversupply of IT people in the country and that, in regard to migration, we should be putting a stop on people who are coming in on extra points because of that. Do you think that that is a factor?

Mr Henley—Yes. There are a lot of IT people who are currently looking for employment. I find that we have employed two types of people in PricewaterhouseCoopers. We had the philosophy that we would bring in people who have law enforcement experience and an interest in computers. That has worked particularly well because they innately, from their law enforcement experience, have a concept of continuity, brief preparation, evidence, the court system et cetera. We have also brought in people who have straight technical skills and have tried to teach them the computer forensics or the investigation skills. That has not been so successful. It has worked in individual cases but, generally speaking, it has turned out better for us to grab the IT people with an investigations background, which is why we have looked predominantly to law enforcement in the past.

Senator HUTCHINS—Have you employed hackers?

Mr Henley—No.

Senator HUTCHINS—Do you have a policy against employing them?

Mr Henley—I have arrested and interviewed a lot of hackers over the years, and it is my personal view from talking to the people and seeing the types of people who have actually been employed by organisations to do such things that I would not go near them with a barge pole.

Senator HUTCHINS—I think that it was on Friday that Symantec said that some of the people in that industry do employ hackers. They said they would not.

Mr Pobihun—Is that within computer forensics or within tech. security management? They actually use quite different skills.

Senator HUTCHINS—It could be either.

Mr Pobihun—One thing that I think should be remembered throughout this discussion is that a lot of the training that we get from the United States is technical but there is very little presentation of evidence skills training. You may learn how to use the tool in case of whatever but you are not going to learn how to present your findings in a court of law.

CHAIR—Do you think—especially Mr Henley, who has been in the law enforcement area himself and is now in the private sector—that there is a lot of turf warfare in terms of who is actually responsible for cybercrime? Do you think that it should be centralised more than it is, with the one body?

Mr Henley—The benefit of centralisation is the ability to get over the issues of jurisdiction. When one body gets to talk to one body in the different parts there is greater transfer of information. When you have a New South Wales Police computer crime unit and a Federal Police computer crime unit you start to get issues of whose case it is and the transfer of information. If we could have everything our way, I would like to see a global cybercrime unit that was able to access information globally without any problems. That is a bit of a fantasy perhaps—

CHAIR—It sounds fair enough.

Mr Henley—but moving to a single body really addresses some of those issues and allows information to flow much more effectively.

Senator HUTCHINS—Does the current regulatory environment address the problems of detection and enforcement, in your opinion?

Mr Pobihun—The very nature of the beast suggests that it is impossible to detect every activity. All of our work is reactive. We cannot go in and investigate until somebody raises the issue. We are currently looking at new technology that will provide us with more proactive investigation skills. However, that is for the big end of town at the moment. It is a very expensive package and a very specialised tool kit.

CHAIR—Thank you very much for that input today. It has been very useful, especially coming from somebody who has looked at life from both sides now. That was excellent—we appreciate it.

[3.57 p.m.]

BANNERMAN, Mr Bruce, Principal Legal Officer, Funding and Assets of Crime Section, Criminal Law Branch, Attorney-General's Department

CLEMENT, Mr Trevor, Assistant Secretary, Critical Infrastructure Protection, Attorney-General's Department

McDONALD, Mr Geoff, Assistant Secretary, Criminal Law Policy, Attorney-General's Department

ROTHERY, Mr Michael, Director, Critical Infrastructure Policy, Critical Infrastructure Protection Branch, Attorney-General's Department

SCHNEIDER, Mr Anton, Acting Assistant Secretary, Strategic Law Enforcement Branch, Attorney-General's Department

WILLIAMS, Ms Kelly, Principal Legal Officer, Criminal Law Branch, Attorney-General's Department

CHAIR—Welcome. I am very glad you could come today. You are the last people we are talking to in this inquiry and are obviously a key group. I call the committee to order and declare open this public meeting of the parliamentary Joint Committee on the Australian Crime Commission. The committee is examining recent trends in practices and methods of cybercrime with particular reference to, firstly, child pornography and associated paedophile activity; secondly, banking, including credit card fraud and money laundering; and, thirdly, threats to national critical infrastructure. The committee, when it reports, wishes to be able to provide a picture of the emerging trends in cybercrime and offer guidance as to the role the newly established Australian Crime Commission might play in combating this crime. As you know, we prefer evidence to be given in public. If you wish to go in camera, please advise us. We now invite you to make an opening statement. With six experts we feel somewhat outnumbered, but we look forward to your evidence today.

Mr Schneider—The department's submission provides an overview of Commonwealth initiatives to counter the various aspects of cybercrime. As you know, representatives of the department are available today to clarify various aspects of the submission. Commonwealth initiatives to counter cybercrime fall into three main areas: protection of the national information infrastructure, strategic law enforcement policy developments and development of appropriate legislation. I am available to provide information in relation to law enforcement policy aspects, Mr Macdonald will provide information in relation to criminal law matters, as will Ms Kelly Williams and Mr Bruce Bannerman. Mr Trevor Clement and Mr Michael Rothery are available in relation to critical infrastructure issues. If the committee agrees, I would like to read a short statement in relation to law enforcement policy—strategic law enforcement policy.

CHAIR—Okay.

Mr Schneider—In relation to law enforcement policy, since the department's submission was lodged at the beginning of June 2003, there have been a number of further developments. I would like to take this opportunity to outline them. On 6 July 2003 the Minister for Justice and Customs, Senator Ellison, announced a major government initiative to combat ID fraud. This development was anticipated on page 12 of the department's submission, which indicated that the Commonwealth was coordinating work to address ID fraud and theft from a cohesive whole of government perspective.

The whole of government study announced by Senator Ellison will test the feasibility of three studies. The first is an online identity verification service for primary identification documents. The study will outline and analyse key factors requiring consideration in the development and implementation of a document valuation service. The second study is to identify and reach agreement on a common set of identifying documents of higher integrity to be used by Commonwealth agencies for purposes of identifying clients. The third is the development of proposals for more well-defined cross agency data matching to detect fictitious identities and cleanse identity registers. The aim is for the timetable of the three feasibility studies to be well-progressed by later this year—probably by October. The studies are being conducted by a Commonwealth reference group comprising some 20 Commonwealth agencies. It is envisaged that separate steering committees will be established for each of the three studies and work currently undertaken by other agencies will be incorporated into this process.

In relation to credit card skimming, at the last meeting of the Australasian Police Ministers Council on 2 July 2003, all state and territory police ministers endorsed the national approach to card skimming and supported Commonwealth initiatives to improve the collection, correlation, analysis and dissemination of intelligence on skimming and associated frauds and the development of model skimming offences. Those initiatives are outlined on page 11 of the department's submission. Model card skimming legislation is currently being developed by the Model Criminal Code Officers Committee in consultation with the SCAG-APMC joint working group.

Some jurisdictions deal with credit card skimming under the broader issue of identity theft or fraud. MCOC will consider whether model card skimming offences should be incorporated as part of a package of wider identity theft offences. The target date is the next meeting of the Australasian Police Ministers Council on 11 November 2003. The first of this year's biannual ministerial meetings with financial institutions to discuss fraud—in particular banking fraud—was held on 14 May 2003. Following that meeting, further cooperation—and information and intelligence sharing—between the banking sector and law enforcement agencies has occurred.

The last issue is a national approach to child protection offender registration. As anticipated on page 10 of the department's submission, the concept of a nationwide child protection offender registration system was considered at the 2 July 2003 meeting of APMC. APMC endorsed the development of complementary state and territory police administered child protection offender registration schemes. CrimTrac has been tasked to develop a report for APMC on the preferred concept of operations for a national register system and a business case by the end of September 2003. A number of questions relating to the concept of a national registration system will also be the subject of further consideration by working parties of the APMC and the Standing Committee of Attorneys-General.

Mr McDonald—I might take up the issue of computer offences. A key part of our strategy has been to have modern and updated offences, and these were enacted in 2001 as part of the Cybercrime Act. Those offences were developed in cooperation with the states and territories and, like all the other measures that have been outlined, there was public consultation. Those offences are part of the focus of the Leaders Summit on Terrorism and Multijurisdictional Crime. So far the Commonwealth has enacted the offences, as have New South Wales, Victoria and the ACT. The Northern Territory has substantially enacted the offences. What we are moving to is consistent offences across the country, recognising the cross-border nature of this type of crime. When developing the Cybercrime Bill we took into account the Council of Europe Convention on Cybercrime, to make sure that we developed those offences with an eye to what was happening internationally.

The situation is always changing with this area of legislation. The old offences were only 10 years old but they might as well have been a hundred years old because in 10 years so much occurs in terms of the technology developing and the terminology losing relevance. That is something that we have attempted to avoid with these new offences. Instead of confining them to technical terms, we have tried to more describe the misconduct, though we will have to be very vigilant about the continued relevance of the offences.

The offences cover not only conduct which affects a computer system such as a denial of service attack but also unauthorised use of a computer to facilitate commission of another serious crime, such as hacking into a bank's computer and committing fraud. The Cybercrime Act also included some new criminal investigation powers. These could only be exercised where there were reasonable grounds to believe that the electronically stored data might constitute evidential material within the terms of a search warrant. The powers included powers of compulsion to assist in getting access to the computer and the ability to investigate links which might have information on another site, so you could have a computer which does not actually have the information stored on it but just has links to these little sites. There were also enhanced powers to move the computer equipment off-site.

We need to bear in mind that with the Criminal Code theft-fraud offences, which are fairly recent as well, in the year 2000 we updated concepts of forgery to take into account new technology: smart cards and that sort of thing. One of the things that we are looking at, which Mr Schneider mentioned, was credit card skimming and the whole idea of perhaps an identity theft offence, which is a species of theft-fraud offence that we are looking at in terms of making those offences easier to deal with.

Finally, the Internet has been used to obtain and distribute child pornography, and there has been quite a lot of concern about this. The government has announced it will introduce new offences and will provide a nationwide avenue to investigate, prosecute and punish those who use the Internet for trade in child pornography. These offences would carry a maximum penalty of 10 years imprisonment, which would line up with the type of penalty that would apply for bringing in hard copies through the customs barrier. We expect that that bill will be released as an exposure draft within the next month or so, and it is on the agenda for introduction in the spring sittings. That will be an interesting piece of legislation. We hope that a discussion paper on credit card skimming offences and identity fraud offences will be circulated for public comment in spring.

We found with the computer offences that value of public consultation was just incredible. We are very strong believers in that, particularly in technical fields. One of the things I am very pleased about is the way in which the computer offences have quite a bit of technical credibility. It really came out in the Senate committee hearings, so we are very conscious of the need to make sure that those that are very aware of these issues have an opportunity to comment on it. The paper will be released by the model criminal code committee, and that should be an interesting development. If you have any questions, I would be happy to answer them.

CHAIR—Thanks very much for that; that is comprehensive and also provides quite a useful reference in the *Hansard* for us as we go through it. There seems to be a proliferation of organisations that are involved in cybercrime. Do you think there should be greater centralisation with one body? If so, which one? Do they need more resources? How can you complement that? Also, would you see your role as continuing on with policy? There is a view that the High Tech Crime Centre is basically operational without developing policy per se. Should it be given some policy grunt as well or, if the interface with your department is sufficient, is that necessary? So that is it, firstly—in terms of the general question of turf warfare.

Mr McDonald—My colleague here may be able to comment more on the law enforcement agency type connections but, in terms of the input of agencies into the policy process, we have certainly found that law enforcement agencies are more than able to come up with suggestions in relation to their powers and the offences that might enhance their capacity to deal with those who harm others, either their property or personally. However, there are many issues that are touched by these laws, including privacy issues, their relationship to other theft and fraud laws, other property damage laws and there is some value, I believe, in the departments of state continuing to play important roles in ensuring that there is a balance of the various interests.

The departments of state, particularly in the need to cooperate with the state and territory governments, are able to conduct consultations which I hope the community would consider fair and reasonable. So there is some value in having the policy aspects separate, particularly in relation to the legislation. That does not mean of course that the whole policy process is not benefited by the fact that these agencies develop some policy capacity. We have particularly found this in the area of money laundering and cross-border crime. We have found that the Australian Crime Commission and its predecessor, the National Crime Authority, have made a valuable contribution to the development of, say, the proceeds of crime legislation and money laundering offences.

I do not know whether others will want to comment on the law enforcement agencies. The nature of cybercrime is such that it does raise its head in just about every area of criminal endeavour. One of the reasons you have so many people here today is the fact that it does impact on so many different areas. I think that state police forces have a very important role in all this, as well as the federal agencies. There is some value in the diversity, in the sense that different agencies are focusing on particular aspects. So, in terms of centralisation, obviously there will be a real value in the high-tech area in drawing together the skills that are needed to really focus on this area of crime. However, it is important that everyone is conscious of cybercrime in all agencies.

CHAIR—It is quite interesting that at the state level there seems to be strong interest in having it centralised, for what it is worth. You apparently are producing this national child sex

offenders register, which I think is a good idea. As part of that, would there be some benefit—whether this be federal or state—in monitoring their access to computers during their probation, or for even longer? Has any attention been given to that?

Mr McDonald—I am a little bit confused.

CHAIR—I am talking about when a child sex offender comes out of jail. One of the comments that was made was: 'If you're really wanting to look at the most likely people who are going to be involved in accessing the computer to send child pornographic images, abuse the chat rooms et cetera, then look to those who have already been convicted of child sex offences.' So, when people are let out of jail on probation and we have got their names in the register, should we have an ongoing monitoring system or some censoring device on their Internet usage?

Mr McDonald—I think the register will aid the police in doing that type of thing, though obviously how they do it operationally is something they would answer better.

CHAIR—You are the last one in. There have been some suggestions about the ease in which they are able to, in their own homes, go into grooming—and then you never know until it is too late.

Mr McDonald—That is right. There are criminal history records already available to the police, but the child sex offenders register will enhance their capacity. It is particularly important that the local authorities are aware of people who move into an area so they can provide adequate protection. But, in terms of getting into the operational nitty-gritty of the best way to do it, I imagine it would vary depending upon the circumstances. The aim of the child sex offenders register is to ensure that local knowledge of who is coming into the area is enhanced so that the police can take the necessary measures. I am sure that, if there is some indication as to who the person is when they are monitoring what is happening in chat rooms and so on, then there would be a connection, but of course people use false identities and the like.

CHAIR—The suggestion came up when we were in Sydney about regular police monitoring of chat rooms. It already goes on on an ad hoc basis, as you would be aware. In doing so it is like driving an unmarked car through a patrolled area. That gives you some information, but if it is known then perhaps those who regularly use it would use more caution.

Mr McDonald—I had the pleasure of attending a briefing from the police about two months ago and the Queensland police were able to give me some idea of how they go about this. Certainly it is something that has been occurring in that state. Just from what I saw—and you would be really better off getting evidence from the police directly on this—it seemed to be an effective measure. They were able to point to specific cases where this had been very effective. In fact, quite often, where the predators thought the person was a young child or something like that, they seemed to be attracted in very large numbers.

CHAIR—Do you believe that there is a need by legislative means to ensure that records from the Internet service providers are held?

Mr McDonald—That is a matter that has been debated for some time. It is something that I am well aware that law enforcement agencies have wanted, but really the communications

minister and that department are the people who should be commenting on that. There would of course be some administrative burden on those organisations while, on the other hand, there is quite clearly some law enforcement advantage in it.

Mr SERCOMBE—Given the international nature of cyberspace or whatever we want to call it, what sorts of mechanisms were involved for the Commonwealth in terms of achieving a number of objectives—looking at harmonisation, perhaps in areas of principally economic interest, in information technology with best practice elsewhere, while at the same time ensuring that there is an adequate regime of regulation from an Australian national point of view? I am thinking of things like money laundering in the commercial area. If you go across to the criminal area, it is things like the application of mutual assistance arrangements between Australian criminal jurisdictions and those overseas in a cybercrime environment. I am wondering what sorts of general mechanisms from a policy point of view are in place and whether you are able to talk about their adequacy?

We did have a proposal earlier today from someone who has been involved in law enforcement in Australia that, given the rapidity of movement and development in these areas and given the crucial importance of the international dimension both at commercial levels and at criminal justice levels, it almost warrants Australia considering a cyber-ambassador, if you like. We have ambassadors for refugees and for terrorism and all sorts of other things. Is there scope for focusing the Commonwealth's attention internationally in these areas by giving it a very specific focal point and impetus?

Mr McDonald—It is true that to date the international aspects have been to some extent compartmentalised in relation to particular topics. In relation to money laundering, financial transaction tracking—which my colleague here has been working on—has been dealt with by the Financial Action Task Force. On that particular issue there has been quite significant standardisation of requirements in relation to dealing with suspicious transactions and the like, monitoring transactions between financial organisations around the world. Of course, with the connection of these activities and terrorism there has been a new emphasis on that.

In my opening about the offences, I mentioned that we were very conscious of what was happening in the Council of Europe. We knew that Canada and the United States, as well as many European countries and other countries, were using that particular program to try and harmonise the offences. There is absolutely no doubt that we need to have consistent strategies within this country, which is always a challenge in itself, with our federal system, as well as with those other countries. As for centralising it absolutely under one person, I think there is evidence that the existing mechanisms are working fairly well. My colleagues would probably be able to say a bit more about the technical side of things. Clearly there is a lot of briefing on techniques and developments from the likes of Interpol, the FBI and organisations like that.

Mr Rothery—In addition to there being a range of law enforcement cooperative efforts there are a range of e-security cooperative efforts. The nuance there is that the e-security side is fairly much based on prevention—actually dealing with the owners and operators of systems to ensure that their systems are adequately protected and that they are aware of what threats are out there. Our concern in the region was that a number of emerging economies in the region did not have a strong public policy for actually monitoring the health of their Internet. A case in point would be one of the major viruses that hit the West a few years ago, the 'I love you' virus, which came

from the Philippines. The Philippines had developed some Internet security monitoring facilities that were set up within the academic community, but they had fallen over due to lack of support. As a case study, that has been a very strong lever for the work that Australia has taken a leadership role in, very much with the support of the US, Canada and Japan.

We now have a commitment through the APEC leaders statement from last year that cybersecurity will be seen as a priority for the APEC member economies. In particular, the effort that we have sponsored there is a capacity-building project running in the Philippines, Vietnam, Thailand, Papua New Guinea and Indonesia. It is being run out of the Attorney-General's Department, with the assistance of AusAID funding, to create computer emergency response teams in each of those economies.

Since that proposal got up—and we began work on that earlier this year—APEC has followed suit with funding to pick up the other APEC emerging economies that are not in Australia's immediate region, such as Chile, Peru and the Russian Federation. What we have now are a number of efforts inside APEC to ensure that all governments are monitoring the health of their Internet, that they have cooperative information-sharing regimes between them and that they have an interface with the law enforcement community for the escalation of significant events that may require law enforcement investigation.

Mr McDonald—That 'I love you' virus incident reminds me that, when we put our offences together, we made sure that they had extraterritorial coverage so that, if an Australian chose to perpetrate something by just going off to an island country that did not have adequate laws or something like that, our offences would cover that.

Mr SERCOMBE—In relation to other aspects of our legislation, I think you yourself said, Mr McDonald, that things move so rapidly that legislation becomes outdated quite frequently. Look at the Financial Transaction Reports Act 1988, for example—it is pre Stone Age in cyberspace terms. I guess there are other areas of legislation as well. Is there a mechanism within the department for scrutinising the ongoing adequacy of an important piece of legislation like the financial transactions act?

Mr McDonald—The financial transactions act is an example of legislation that we have done extensive work on over the last 18 months. My colleague Mr Bannerman is developing a major proposal for the updating of that act. The updating of it is of course being done in tandem with the updating of the international standard. There are 40 recommendations from the Financial Action Task Force, and these are being updated in the light of new developments and new types of financial organisations. I do not know whether you would like to add to that, Bruce.

Mr Bannerman—The Financial Action Task Force has only very recently—in fact in mid-June—agreed on a replacement set of anti money-laundering principles. Those principles are reflecting quite rigorous new standards that are going to be required, for example, in relation to customer due diligence, identification and verification, which will link in with other sorts of processes which are going on in other areas of the department and agencies. This is going to mean quite substantial amendments to our act. We are just at the start of that process now and government decisions have yet to be made on the detail of it. This will be Australia's updating of our legislation in accordance with the international standards. Those amendments to the 40 principles have been very extensively considered by the international Financial Action Task

Force over the last 18 months or two years, and Australia has been a player in those negotiations and discussions.

Mr SERCOMBE—Are you able to give us some illustrations, perhaps some examples, of issues that have emerged in recent times which you will be picking up in the review—things like e-gold, for example, and Internet based currency issues?

Mr Bannerman—I cannot give particular examples because final decisions have not been made on the form of the act, but the sorts of things that financial players will have to do now before they can undertake transactions will include substantial prudential type requirements. One of the interesting developments that the task force is requiring financial institutions to do is to incorporate into their general prudential requirements anti money-laundering principles rather than seeing it as a separate exercise. So over time that is going to change the culture of this sort of oversight by institutions.

Mr McDonald—The difference with 1988 that you mentioned before is that so much of the community's financial transactions were done through this banking system. There are so many different types of financial institutions now outside the banking area, as well as organisations doing their own in-house transactions which are quite significant. With everything from charities through to the non-banking financial sector, the whole range of organisations that are now involved in international transactions is much broader than existed then, when it was under the almost exclusive control of the banks.

What was great about 1988 was that Australia developed legislation at the time when computers were being brought in on a large scale in the banks, and so we had the first really computerised reporting system. We were at the leading edge on that. Because those big institutions could afford that infrastructure, at the beginning it was a very effective system because so much of the financial transactions was through it. But as time has gone by there are increasing areas of financial transaction that are outside that system and where sometimes they do not have the same infrastructure as the banks, which makes the reporting processes more difficult. That is going to be the challenge which will come through the consultation process on this legislation, to make sure we have legislation that is both effective and at the same time not imposing too crippling a demand on the organisations.

Mr SERCOMBE—I understand it requires you to go to government, but, allowing for that unpredictable aspect, are you able to indicate what time scales we are talking about here? Are we talking about the end of this year or next year?

Mr McDonald—The time scale is in that sort of range. We will have a consultation process. I would expect that it is something that will be occurring over the next six to 12 months.

Senator GREIG—I want to ask a question about privacy. I was wondering if you could paint me a picture of where policy is driven from in this regard. It seems to me that we have three areas of government authority that in some way address this: seeing as we are dealing with cybercrime and Internet crime, we are dealing with the National Office for the Information Economy, with A-G's in terms of the law and, overriding that, the Privacy Commissioner. To what extent do they interact, if at all? Where is the policy push and the agenda set from the

government side of things and from the department's in terms of addressing privacy issues and monitoring them?

Mr McDonald—In the Attorney-General's Department—whether it is on the crime side, which is my side of the camp, or the civil justice side—there is a great consciousness of privacy issues, both as a department of state within our department and also in our relationship with the Privacy Commissioner. Our relationship is close, and we recognise that he has a statutory role in this area in advising on legislation. On the crime side, whenever you look at adjusting police powers or adjusting offences it is quite amazing how many privacy issues are raised. The Privacy Commissioner interacts regularly with our ministers and makes suggestions which are taken up in our policy work. I have worked on everything from the DNA database system through to this recent exercise where we have discussion papers out on the appropriate legislation for electronic surveillance and controlled operations, those sorts of issues. There is continuing discussion with the Privacy Commissioner about those issues.

The Privacy Commissioner is a significant influence in his own right. Our department is very strongly committed to ensuring that there is a proper balance. I think you would find that NOIE and the communications department would be pretty conscious of the same sorts of issues because the people they work with are very conscious of them too. The police, to their credit, have an understanding of these issues. They know that the mishandling of information could cost people their lives. I have actually found that the law enforcement agencies have a more acute consciousness of these issues than a lot of people would think, though in the balancing act obviously the law enforcement agencies are very keen to gather as much intelligence and evidence as they can to prove a crime.

In the criminal law branch we assist in developing laws which enable efficiency but at the same time make sure that that is not at the cost of people's ability to go about their everyday lives. It is a very difficult process. You have to design safeguards carefully so that you do not create a practical web which, if anything, encourages noncompliance. You need to develop safeguards that have a real impact and at the same time are simple to use. That is a continuing challenge for us, and the Privacy Commissioner has been very helpful with that.

Mr Rothery—From the e-security point of view, we see privacy as being a major driver in encouraging adequate protection of customer and other personal records that industry have. In developing the arguments for enhanced e-security by organisations we quite often use the example of privacy—being able to enhance the surety of the privacy of individual data. We have both the information law and the e-security functions within one division. We see them not as being in conflict but as achieving a mutual objective.

Senator GREIG—Would the child sex offenders register be based solely on those people who have been convicted and served time in jail, or more broadly?

Mr McDonald—It focuses on people who have been convicted.

Senator GREIG—So that would include a jail term?

Mr McDonald—Yes, it would. Usually with those sorts of offences people do get some imprisonment. In the event that they were convicted but released on a good behaviour bond or

something like that, they would be caught too, but for child sex offences people do get jail. The most important thing is that they are people who have been convicted. There is a Western Australian study which shows that the level of reoffending in that area is pretty frightening.

Senator GREIG—I am asking in the context of the differential ages of consent we have around the country, both between states and between heterosexual and homosexual behaviour, which create a bit of a dog's breakfast in definitions when you are dealing with sex offences. In my home state of Western Australia, until only a year ago consenting gay sex was a criminal offence until the age of 21. If a 20-year-old gay man was in a consenting relationship with a 22-year-old gay man, the older gay man in that relationship could be charged with sexual offences against a minor. It was an absurd situation, yet I know of people who were prosecuted—and in some cases jailed—under that legislation. I am wondering whether this kind of anomaly is taken into account in the formation of this legislation and the register.

Mr McDonald—The good news is that, as you point out, in the last five years there has been a big move towards more similar ages of consent around the country. Western Australia is one example. New South Wales, Tasmania and South Australia are others. Of course, Tasmania and South Australia have moved to a non-discriminatory system in which the age is 17. Yes, the system will take that into account. While the details have not yet been released, we have taken that into account. I am a bit reluctant to say exactly how we have dealt with it, because the details of the scheme have not yet been released and we have worked on it with the states, but I can tell you that there has been some sensitivity to that issue.

Senator GREIG—My particular concern is that I would not like to see a situation where somebody appeared on the register because some years ago they were convicted under essentially anti-gay laws—discriminatory age of consent laws, which for the most part we have now dealt with as a nation—and not because they were genuine sex offenders.

Mr McDonald—Yes. That is a very good, important point. I think you will find there is some sensitivity to those issues.

CHAIR—We have heard quite a bit about possession. When does it become an offence—when you open the email, when you receive it, when you download it, when you store it? That seems to be a terribly grey area. There is a lot of apprehension and discussion about it in the various submissions we have received and in the evidence we have heard.

Mr McDonald—We are developing—and Kelly may want to say something on that—the offences right at this moment. Certainly possession is all about control.

CHAIR—Are you going to put in intent? We had Electronic Frontiers talking about that. I do not know if you have met them.

Mr McDonald—We have read that. These are quite serious offences. Under our Criminal Code, serious offences require proof of fault, so we will have appropriate fault elements—there is no question about that.

CHAIR—Just receiving spam which contains pornographic imagery is one thing.

Mr McDonald—Yes, you are right. Innocent people could be criminalised. Our whole focus in the Criminal Law Branch is making the criminal law focused and not unduly criminalising too broad a group of people. Our system is one where we try not to rely too much on prosecutorial discretion but to ensure that the legislation gives some clear direction on these matters. The provisions that we are developing I cannot give to you yet, but it is not that far away. As soon as we have the exposure draft—

CHAIR—Obviously that is highlighting the fact that that is an area we are concerned about—we might want to talk about that.

Mr McDonald—We have come here today having read the Electronic Frontiers submission, and we are conscious of that issue.

CHAIR—It would be quite useful to look at the evidence that was presented today. The only other one I had was related to section 25A of the ASIO Act—the powers of compulsion and so on—and whether they would be used in terms of cybercrime issues and whether they could be said to be in the national interest.

Mr McDonald—There is a big difference between security legislation and law enforcement legislation, which we would have to go through very carefully. Security legislation is primarily about preventing something from happening, taking some sort of immediate action to prevent the problem. Law enforcement legislation has a much longer term impact. It impacts, in some cases, in terms of whether a person gets a conviction and gets imprisoned for a long period of time. So we have to be very careful about extending powers that are for security agencies across to the law enforcement side of things.

CHAIR—But you can see areas where it can overlap in terms of cybercrime—threats to water supplies, electricity et cetera. The security of the banks could also be questioned.

Mr McDonald—Yes. The issues you are talking about are a major sort of tension that is being looked at and has to be resolved. I have mentioned in a policy setting why our laws are like they are. We are continually looking at it and asking, 'Is there more that can reasonably be done in terms of the law enforcement powers?' It might be that there can be some adjustment of the law enforcement powers; appropriate safeguards and appropriate limitations might make it acceptable. But the circumstances are quite different, and I can tell you that this whole area is one that will be looked at very closely. You know of course of the history of telecommunications interception legislation and the great care that has been taken with that.

CHAIR—That is right.

Mr McDonald—There is not a big leap between that and intercepting computers and electronic surveillance, bugs and things like that.

CHAIR—And phones. Another problem we have talked about as well which we have not addressed here is taking photos and transmitting those from phones.

Mr McDonald—Yes. There was an interesting article in the *Canberra Times* on the weekend on that. It is an interesting dilemma. In some ways taking photographs is the sort of thing that

has been going on for a hundred years. We have to conceptually think carefully about whether we are really dealing with something new or whether we are dealing with something old. There are some challenges there.

CHAIR—We have to catch flights. I would have liked to have gone on because at the end of the session there are a lot of things we could talk to you about. Anyway, we will be in touch as we work through some of these issues. It was a three-day inquiry, which is fairly brief. It has raised a number of issues which we would like to work through, especially in terms of some of the recommendations.

Mr McDonald—If there is anything you would like us to provide, any further information, we are more than happy to do so. You can see from all our activities that it has been a very large area of activity for the last few years. But, as I said earlier and I think was agreed by Mr Sercombe, it will continue to be something that we will have to monitor because the technology is developing so quickly.

CHAIR—Thank you very much for coming. Thanks for the input. We will be in touch with you.

Committee adjourned at 4.57 p.m.