COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE ON THE NATIONAL CRIME AUTHORITY

Reference: Law enforcement implications of new technology

FRIDAY, 2 MARCH 2001

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

INTERNET

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

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

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

JOINT COMMITTEE ON THE NATIONAL CRIME AUTHORITY

Friday, 2 March 2001

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

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

Terms of reference for the inquiry:

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

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

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

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

WITNESSES

Committee met at 9.35 a.m.

GRABOSKY, Dr Peter Nils, Deputy Director, Australian Institute of Criminology

URBAS, Dr Gregor Frank, Research Analyst, Sophisticated Crime Program, Australian Insttiute of Criminology

CHAIR—I declare open this third public hearing of the Joint Parliamentary Committee on the National Crime Authority inquiring into the law enforcement implications of new technology. We are also having a public hearing in Sydney next week. We are starting today's public hearing with representatives from the Australian Institute of Criminology and I welcome you both, gentlemen. Your fame has obviously attracted much attention to our committee because I understand that for the first time we are going out live on the Internet.

Dr Grabosky, I understand that you gave this committee the benefit of your expertise in relation to the electronic commerce issue back in March 1997, although some of the members of this committee will have changed since then. We have noted your long-term interest, we have read some of your books with interest and we are grateful for you giving us your time today. The committee prefers that all evidence be given in public but you may at any time request that your evidence, part of your evidence, or answers to specific questions, be given in camera and the committee will consider any such request. We have received your submission and it has already been published. I would invite you now to make an opening statement.

Dr Grabosky—Thank you. We at the Australian Institute of Criminology began work in this area in early 1995, culminating initially in the publication of a book entitled *Crime in the Digital Age*, which was published in February of 1998. Since that time my colleague Russell Smith and I, in collaboration with Dr Gillian Dempsey of the University of Queensland, have published another book entitled *Electronic Theft: Unlawful Acquisition in Cyberspace*, a copy of which my colleague Greg Urbas has just shown you. That was only printed last week and its release is pending by Cambridge University Press. In addition, my colleagues and I have published a number of papers in our Trends & Issues series, which are all available online at the Australian Institute of Criminology web site. I have copies of our bookmark to that web site here if anyone is interested.

We have also published material in various academic journals and, in addition, engaged in various consultancy activities for both public and private sector clients. One engagement involved some work we did for the Health Insurance Commission on risks attending the movement to the electronic environment. An abridged version of that has been published in the Trends & Issues series. In addition, at the moment we have been engaged by the Confederation of Asia and Pacific Accountants on a project relating to business-to-business fraud in the Asian region. My colleague Greg Urbas is working on that at the moment.

I should mention that we share the results of our research with government departments as we produce it. The *Crime in the Digital Age* book was presented in draft form, chapter by chapter, to the Attorney-General's Department many months before its ultimate publication. Similarly, the day that it was sent for editorial consideration to Cambridge University Press—which was about a year ago—the *Electronic Theft* book was circulated to the Attorney-General's Department, to the Australasian Centre for Policing Research and to AUSTRAC, among other

agencies. So we are very happy to share the results of our research well in advance of publication with various government departments. I should mention that in addition to our published work we have links with the United Nations. It was my privilege to serve on the Expert Working Group on Crimes Related to the Computer Network under UN auspices last year.

There are four issues that I would like to raise regarding the context of computer-related crime, and I will just raise these very briefly. The digital age that we are now in has provided us with unprecedented opportunities for enrichment in many, many areas of life—for example, education, communications—tremendous opportunities to develop commerce and economic development generally. At the same time, digital technology, as you know, poses significant risks. The challenge is to maximise the benefits of digital technology and allow for prosperity in cyberspace while minimising the downside risks of these technologies, specifically their criminal exploitation. There is no perfect solution to this. Zero tolerance of computer crime would be massively expensive to implement, arguably impossible to achieve, and would occasion significant opportunity costs and collateral damage. That is, the more burdens you place on Internet service providers, or the more difficult you make it for people to access information systems, the less are the opportunities for the positive upside of digital technology to flourish.

The second theme I would like to touch on briefly is what one might describe as the fiscal crisis of the state. You would all be familiar with relentless pressure to reduce public expenditures that governments throughout the world are facing as a result of the globalised economy. The third, which flows logically from the second, is that police are required to do more with less. This has posed very significant challenges to law enforcement agencies who now have more work than they can handle. This is particularly apposite in the domain of computer forensics where, in addition to the growth in business for those who would investigate computer-related crime, there is what one might describe as a brain drain—that is, just as a police officer becomes skilled in computer forensics they are often able to improve their salary significantly by moving to the private sector. So one has seen routinely in most law enforcement agencies—in the English-speaking world at least—a movement from the police service into the private sector. This, of course, entails significant costs in skilling up new members of the police service. Whether this brain drain will endure or whether it is a transitory phenomenon until computer literacy becomes more widespread is an open question. Suffice it to say, for the time being this brain drain is a significant issue for most law enforcement services.

Finally, I make the observation that cyberspace knows no borders. As you are aware, offences can be committed from the other side of the world and this means that it is a global problem quite often, and global problems require global solutions, or, at the very least, national solutions. This suggests that law enforcement agencies should coordinate and/or rationalise their activities rather than each re-invent the wheel. There are some efficiencies that can be achieved through concerted action and one suggests that they should be so achieved.

A final observation is that law enforcement agencies should stick to their core business, which is law enforcement investigation, and I would like to suggest that, rather than do their own research, law enforcement agencies might articulate their knowledge needs and let researchers address them. That concludes my initial remarks.

CHAIR—Thank you, Dr Grabosky. Continuing on that theme about the internationalisation of the problem, could you perhaps tell us how successful international law enforcement cooperation has been in this area to date? Have there been any particular successes and what are the reasons why there might have been those successes? Are there particular problems associated with that cooperation? I suppose the ultimate question is: is any cooperation that is taking place, however successful it may be, ever going to extend to what you might call 'real time' cooperation?

Dr Grabosky—There has been a significant movement towards the harmonisation of laws internationally and towards improvement in law enforcement cooperation internationally. I think the Group of 8, as it is now called, and the European Community have made the most significant strides in that direction by identifying the core elements of laws to combat computer-related crime, and also the establishment of 24-7 contact points—that means people in law enforcement agencies in each participating state or nation who can be available on a 24-hour, seven-day basis—to address that second point you made about real time cooperation. But the world is a big place and the real challenge is in bringing other nations, particularly those that may be less technologically sophisticated or less up-to-speed basically, along in international cooperation.

CHAIR—So you are saying that if I am a crook and I operate in a Third World country I am much more likely to get away with it than if I operate in a First World country?

Dr Grabosky—I do not think that is an unfair generalisation, tempered, of course, by the fact that the telecommunications infrastructures in some Third World countries may not support the kinds of technologies that you would need to undertake some of the more sophisticated types of offences. There are criminal havens that apply to terrestrial crime as well as to cybercrime and that, as I say, is a pretty fair generalisation.

CHAIR—In your paper *Computer Crime in a World Without Borders*, you posed a number of rhetorical questions. Perhaps you could expand for us on the issues that you think are of particular concern for Australia and what, if anything, we should be doing immediately to try and improve the situation?

Dr Grabosky—I have a copy of that paper here. That was based on the special United Nations Working Group on Crimes Against the Computer Network that I was involved in. The key player in that was a gentleman from the Canadian Ministry of Justice who had been raising these questions in public fora—the G8 amongst them—for some time, and these are questions that people are invited to think about in terms of their application. I am afraid that I do not have the answers to these questions but I have—

CHAIR—That is unfortunate because we are quite good at asking questions but we are looking for some answers.

Dr Grabosky—The way to move forward is to raise these questions in appropriate fora and stimulate thinking about how they might be addressed. I have done this by sharing them with organisations like the Attorney-General's Department and the ACPR as well as more public fora. I think one of the most intriguing questions relates to search and seizure in a transborder

networked environment and I could do no better than to just read a couple of these questions to you now:

(i)Can investigative authorities in one country obtain, directly through an inter-connected computer system, data which exists abroad? Can this data be obtained from a publicly available source? Can data be obtained from private systems or data banks with the consent of third parties who have the right to access the data in the other country, without seeking judicial authority or permission from the other country?

(ii)Does the law of your country permit law enforcement agencies to undertake a trans-border search directly into another country, through an inter-connected computer system? Would your law permit them to do it if they had to break or compromise a password in the foreign country in order to obtain the data? If a transborder search occurs, should a notification be made to the state involved, or to the persons involved?

These are just two examples of—

CHAIR—Those are all the questions that we are looking for answers to. Is there anywhere in the world where people have come up with some solutions to those questions?

Dr Grabosky—Not that I am aware of at present.

CHAIR—Which of those sorts of issues would you rank the highest for Australia to give its attention to?

Dr Grabosky—Of the two questions that I have raised or of the bank of questions?

CHAIR—Of the bank of questions.

Dr Grabosky—I would have to pass on that.

CHAIR—Obviously in the technology area there are problems in terms of the admissibility of technological evidence. As I understand it, one of the problems is in the admissibility of photographs taken with digital cameras. Do you have any information on that?

Dr Grabosky—That is very difficult because of the ease by which digital images can be altered. I would imagine—and I am speaking speculatively at this point because I do not have specific knowledge—that technology exists by which a document could be authenticated, much as the technology of videotaping or audiotaping the statements of witnesses by law enforcement enables a degree of authentication. So I would imagine that software technology exists to permit authentication of digital images.

Senator DENMAN—If the NCA was under investigation by a body other than itself, would you feel happy that they were secure? For instance, if it were an outside body using this new technology, would their privacy be adequately protected?

Dr Grabosky—I am not in a position to comment on the integrity of security systems in place at the NCA. I would hope that the systems they do have in place, in terms of personnel vetting, the quality of locks on the doors as well as their information systems, are secure, but I am not in a position to comment authoritatively on that.

Senator DENMAN—How do you feel about private investigators having access to this sort of technology?

Dr Grabosky—We live in an age where technology is becoming increasingly democratised. I think back a thousand years to when only public institutions and churches held timepieces; gradually the improvement in technology meant that most affluent people could have a timepiece. Now, of course, anybody can have a very inexpensive wristwatch. Similarly, information technology has become democratised as well. When I was born the only computers that existed were owned by governments. By the time I finished my postgraduate studies I had a hand calculator—albeit a very bulky one. Now, of course, the uptake of information technology is very widespread, including strong cryptography.

It seems to me that reducing access to information technology is a solution that has significant downside consequences because it may impede the uptake of technology for legitimate commercial purposes. As an example, there are a couple of states in the world that make it an offence to own a computer or a modem without government approval. This obviously has a chilling effect on the use of information technology for good or ill. It is not surprising to note that these countries are not amongst the world's most affluent. Did that answer your question?

Senator DENMAN—Yes, thank you.

Mr KERR—I was just wondering whether you have any comments to make about the Financial Action Task Force and the interrelationship between that and our law enforcement agencies? Are there benefits of extending some of the activities of FATF across to the tax avoidance area, as opposed to simply money laundering?

Dr Grabosky—I think that the Financial Action Task Force is a good example of the kind of capacity-building and consciousness-raising activities that might be required in the domain of the control of cybercrime. The Financial Action Task Force has been instrumental in assisting some of the smaller nations of the world in developing cash transaction reporting regimes—of course, it was the lack of harmonisation, or the absence of cash transaction reporting regimes, that provided a haven for money launderers around the world. The fact that the Financial Action Task Force is helping raise awareness and helping develop the capacity to introduce these regimes in some smaller countries—which left to their own devices would not be able to do so—is very good and I think that may well be a model for the enhancement of cybercrime control capabilities in nations around the world. I know, for example, that the United Nations at present is giving serious thought to what they might do to improve the capacity for cybercrime control in some of the less developed nations of the world. Vulnerabilities to criminal exploitation are perhaps even greater in these less developed nations which are just beginning an uptake of information technology than in advanced industrial societies where people have been thinking about these issues for some time.

Mr KERR—There are two issues I would appreciate your further comments on. Firstly, FATF has thus far been limited to money laundering; that is, people seeking to disguise the source of funds from criminal activity, usually related to drugs—I think it grew out of the American war on drugs initiatives—and it has not gone into tax avoidance or tax evasion, which, of course, is where international cooperation is quite absent. I am wondering whether you think there is a growing case for it to be extended across into fields other than simply the proceeds of drug crime?

Dr Grabosky—My understanding is that the origin of the ill-gotten gains—or in the case of tax evasion the legitimate income that is not declared—is less important than the structure of identifying anomalous movements of money. That is, it matters little whether the funds in question are the proceeds of drug trafficking, whether they are taxable funds that have not been declared, whether they are funds that have been derived from corrupt payments, or whether they are funds that have been derived from illegal traffic in firearms. The fact that there are funds moving from A to B and then to C and on to D in a suspicious manner, and that the origins of those funds can be identified, is what Financial Action Task Force activity is all about. What matters is that an infrastructure exists to identify anomalous financial transactions. The fact that the initial impetus for this arose from the war on drugs is, I think, irrelevant.

Mr KERR—It may be irrelevant but it is not being used, and deliberately not being used, in relation to those funds which are generated from corrupt investments or from tax avoidance. There is no doubt that FATF is not pursuing those matters.

Dr Grabosky—I am not in a position to challenge that observation. What I am suggesting is that the apparatus exists to address anomalous financial transactions whatever their source. It is like a law enforcement agency that may have certain priorities and disregards other matters. It is not my position to—

Mr KERR—That is okay. I have two points, coming back to the issues that you raised in terms of your papers. The first issue is the question of civil liberties and privacy, and the other, that you spoke of earlier, is the difficulty of law enforcement to retain sufficient competence in the area of high technology investigations. If I could take you to the first point, the question of privacy, there has been a growing degree of concern about some new devices which are being spoken of as having some advantages in law enforcement. One example is an ion sensitive device which replaces sniffer dogs for people passing through customs barriers, through airports or through shops. There is an assertion that these devices can be used in the sense of screening devices for drug law enforcement. There are also suggestions that there are heat sensitive devices being used now that enable you to basically look inside a house and see what movements are occurring without a warrant.

What is the framework? Obviously each one of these things has different consequences for individual rights and privacy so you cannot give a blanket approach, but I suppose you need to think of what a general framework should be for approaching these issues and saying, ‘This is permissible,’ or ‘This is not permissible.’ How do you conceptualise that? Do you have any advice that you can provide us, because obviously law enforcement agencies from time to time will come forward with new requests for our assistance in making those technologies part of the apparatus of law enforcement? An example is that the government has given an indication that it will be introducing a proposal—which I think on its face is quite benign so I am not being critical—which will enable the x-raying of wrist bones to determine the age of people who are either unable or decline to provide their age in order to ascertain whether they are juveniles or over the age of 18. Apparently there is something about the way wrist bones set which occurs around the age of 18 which you cannot see externally but you can through an x-ray.

That is fine, we can look at each thing individually, but what is the framework we should be using in relation to conceding to law enforcement the right to use new technologies? Also, picking up on Senator Denman’s point, I will include not just law enforcement agencies but the

private sector, because the private sector often will put these technologies to work without the kind of constraints that law enforcement is subject to.

Dr Grabosky—Indeed. I devoted chapter 10 of this book to the issue of privacy and focused almost exclusively on the private sector rather than the state as the threat to privacy. Returning to your question, I need not tell you that the basic issue of the balance between the rights of the individual and the interests of law enforcement is one of the key issues of the moment and will be central to the public discourse for the foreseeable future. When I speak to law enforcement agencies I say that this is the key issue of our time. In our democratic society this requires a degree of public debate, and this is occurring and I think that is a good thing. However, there are some aspects where complete open and robust discussion of issues may well reveal one's hand, so to speak, and obviously that requires a great deal of sensitivity, but fundamentally in a democracy open and robust discussions about the powers of the state are absolutely essential. In one of our Trends & Issues papers, entitled *Technology and Crime Control*—published, I think, in early 1998—I introduced what I thought was a good framework for analysing this basic question about a framework for the introduction of new technologies in furtherance of crime control. Obviously, I cannot recall specifically the criteria but I will draw from those which I can recall: effectiveness and cost—of course, by implication, cost-effectiveness is one thing—the absence of collateral damage or adverse spillover is another. But first and foremost of these was the imperative of addressing things openly and publicly and canvassing these new technologies as widely as possible in public fora, the fact that the introduction of new powers be done pursuant to full democratic processes.

Mr KERR—I obviously welcome the idea that we need robust discussion about where we draw the lines, but the question I was really trying to grapple with is whether there is an overarching framework that you might advance that enables us in a sense to conceptualise where you would draw the lines and put that into the public framework.

Dr Grabosky—One of the most important books, I think, in criminology in the past decade is a book by Braithwaite and Pettit called *Not Just Deserts: A Republican Theory of Criminal Justice*. Theirs is a utilitarian argument, and the bottom line is maximum freedom within a society and that encroachments on the freedom of some can be justified if it enhances the freedom of all. I think that is a pretty good rule of thumb. It would argue against using technologies simply because they have come onto the market and require the use of technologies be subject to a cost-benefit calculus, not only in economic terms but also in terms of human freedom.

Mr KERR—That is fine for the public sector where on each occasion where new technologies emerge they usually require legislative consent before they can be used. It is not always the case, but quite frequently there is a public debate and the state is forced to, or chooses to, legislate the framework around which law enforcement agencies can use detection devices of various kinds, and the rules of evidence, of course, in a sense can also be used as a gateway or a barrier to their more prevalent use. But that hardly applies in the private sector, and only occasionally do we have those debates in the private sector. We had them, I think, in relation to listening devices, because the legislation we passed with respect to the authorised use of listening devices for law enforcement purposes went further in most places, and I think comprehensively across Australia now the use of listening devices by private persons is also constrained. There are new technologies—for example, ion detectors or infra-red heat detectors

or a whole range of devices—that, presumably, are not detectable by the person who is the subject of surveillance in the sense that they are not necessarily aware of it, but there would be nothing at the moment that prevents their utilisation, I think, by the private sector.

So in the public sector there is the general principle that the burden of admission of new technologies falls on those who assert that they have a legitimate place within the armory of law enforcement or investigation. In the private sector essentially they go on being used until there is a clamour that perhaps they have gone too far and should be regulated. Is that an appropriate balance? Should there be a different way of dealing with this issue or am I starting at shadows here when I am interested in this question of how we admit or do not admit the use of new devices for surveillance of people in the private sector?

Dr Grabosky—That is an interesting issue, although very complex. I guess the first principle is—and I do not think there is much question about this—that, whatever it is, the technology in question should not have the potential to injure someone. Obviously, you do not want to submit people routinely to radiation, for example. That is an extreme hypothetical, and indeed there would be issues of liability that would flow from that that are terribly problematic. Other forms of scrutiny, such as simple surveillance cameras which are deployed in many private settings, have been subject to abuse—for example, I think video surveillance cameras in a casino somewhere were subject to misuse, and you may have heard about that a few years ago. At the most libertarian extreme, there is the argument that this dilemma is resolvable by market forces. We refer in here to the collection of personal information by commercial institutions—

Mr KERR—Can I just stop you there. How could market forces control the situation where I enter a premises which I do not know has me under surveillance by way of, say, infra-red technologies or by sniffing air around my presence to detect whether or not I use a particular brand of aftershave, let's say—to take it away it from drugs—so that they might market new products to me and what have you? But apparently now these devices exist, I am told. I do not believe they are widespread in Australia but I am told that they are being put in place in other countries for various routine private organisations. Law enforcement, presumably—and this is our inquiry—may in due course say, 'We'd like to have some of these, please, too.'

Dr Grabosky—Returning to the private sphere, a market solution would require either disclosure that a particular system of surveillance were in use or assurances that they were not, and people would then be able to judge for themselves whether the assurances they receive were sufficient or whether the—

Mr KERR—I disclose that I have an infra-red device that is surveilling your street and I know which room in your house you are in. Does market force say that I have to move my house now because somebody in the neighbourhood has decided that they want to watch my intimate lovemaking?

Dr Grabosky—So this is a private—

Mr KERR—Yes, this is my neighbour next door. He has made a full and open disclosure that—

Senator DENMAN—And you can do this without a warrant.

Dr Grabosky—There are ample precedents for the restriction of access to certain types of technologies. For example, take pepper spray: I cannot have a can of pepper spray to protect myself from attacks by stray dogs, although there have been times when I wish I had one. The laws recognise that indiscriminate possession of that technology might have consequences worse than the benefits that free access could provide. One could apply the same to the technology of infra-red surveillance that you mentioned.

Mr KERR—I have probably exhausted that theme but it is obviously one I am starting to become more aware of as people raise with me some of the—

Dr Grabosky—It is not a trivial matter. As I mentioned earlier, the democratisation of technology means that we are going to have access, potentially, to technologies that were previously the monopoly of governments. Another example is that of strong cryptography, which only governments and defence establishments had as recently as 25 years ago. Now anybody can download strong cryptography from the web and—

Mr KERR—At a pretty good price.

Dr Grabosky—This caused initially very great concern on the part of law enforcement interests—indeed, the United States prohibited the export of certain cryptographic products.

Mr KERR—They still do. Coming back to law enforcement and retaining people with competence, the number of people in the law enforcement environment in Australia with skills in these areas seems to me to be quite small. I understand roughly, ballpark figures, the AFP has 12 people for the whole of Australia who are cybercrime experts. Given the dimensions of the issues that you are talking about, that does seem to be a very small node of expertise, putting aside the issue as to whether or not it is being turned over very quickly. Is my ballpark figure roughly what you would expect? I do not know what it is within the NCA, I am not certain of its—

Dr Grabosky—I do not know for sure what the personnel allocations are in either the AFP or the NCA but, from what I understand generally in Australian law enforcement, it is a rather small and specialised group. This, I think, reflects on my earlier observation about the importance of coordination. There have been some good examples of this in other domains of law enforcement—for example, companies and securities—where authorities exchange information on what they perceive to be potentially spurious or potentially criminal investment solicitations online. If the SEC becomes aware of something that appears to emanate from Australia they will contact ASIC, and those mechanisms of coordination I think are pretty good. But if everybody were left to their own devices and the authorities in the Northern Territory were concerned about defending cyberspace you can appreciate that would be a fairly daunting task, because most of the illegalities in cyberspace do not really impact upon the Northern Territory and they would be preoccupied with criminal activities on somebody else's turf. The imperatives of cooperation across jurisdictions, whether they be national jurisdictions or international jurisdictions, are fundamental.

Mr KERR—On the fit of expertise in these areas, there certainly needs to be these cross-jurisdictional links, but there seems to be a question as to whether this area of law enforcement fits within the traditional paradigm of law enforcement and how these units within policing and the National Crime Authority and what have you fit, particularly with the salary structures and

the kind of approach to life that people with those technological skills may have. This is an issue that seems to me to be quite interesting, and in one way we dealt with it when we set up the group that works tracing in Australia—

Dr Grabosky—AUSTRAC?

Mr KERR—Yes, AUSTRAC. We set up AUSTRAC as a separate agency, firstly, because of concerns that otherwise it would be seen as too intrusive and too interlinked with ordinary law enforcement, but secondly, I think, out of recognition that the kind of salary structures and organisational form needed to be different from those of traditional law enforcement. I am just wondering how you suggest we start to think about some of these issues in the law enforcement area as these crimes that you have identified become more bread and butter in terms of the larger responsibilities of law enforcement.

Dr Grabosky—The days are long since gone when law enforcement agencies could present themselves as omniscient and omnipotent. To an ever increasing extent they have had to rely on institutions elsewhere in the public sector, or indeed in the private sector and non-profit sector, for assistance in furtherance of their law enforcement objectives. The challenge of harnessing these non-police institutions, or non-law enforcement institutions, in furtherance of law enforcement I think is one of the great managerial challenges of the moment. It is already happening. This entails various organisational variations on the traditional monolithic entity of a law enforcement agency and the rest of the world. These forms can, for example, involve insourcing of expertise from the private sector. For example, there may be people in the information technology industry whose skills could significantly enhance a particular investigation who may be brought in for that particular purpose on a very short-term basis.

There are various other models of a hybrid for temporary secondments from IT security into law enforcement—for example, personnel exchanges or various variations on the traditional theme of either police or non-police—that I think we are moving towards. I think identifying some of these new organisational forms which can help deliver the goods is a real challenge for law enforcement today and tomorrow.

Mr EDWARDS—One of the things that we are looking at is the extent to which electronic commerce facilitates laundering of the proceeds of crime, and I want to ask whether you could give an estimate of the dollar value of money laundering in Australia?

Dr Grabosky—The short answer is no.

Mr EDWARDS—I asked that question because in the paper *Crime in a Digital Age* there is a figure there talking about underground banking and an estimate of between $100 billion and $300 billion, which is an absolutely staggering amount of money, bigger than the budgets of many countries. I think that is an incredible amount of money. What is the extent of underground banking in Australia?

Dr Grabosky—I cannot speak with authority about that. I know that there are people in the NCA who are studying that in some detail but I have not addressed that personally.

Mr EDWARDS—That was all, except you did say that you did not think that people would want to expose others to radiation. It has already happened in Australia in a different way, just for your information.

Mr SCHULTZ—On the issue of the Attorney-General's portfolio submission, among the many challenges is that the role of government in law enforcement may have a finite limit in the face of new technology and that one part of any future strategy will have to be the education of the informed online consumer. The NCA submission also stressed that, whilst organised crime is international and pays no heed to borders, the NCA itself is still constrained by state judicial boundaries. The extent to which new technology will supplant, or complement, traditional policing methods is another major philosophical issue. Do you wish to comment on either of those issues and do you see technology as more of a threat than a benefit to law enforcement? Are you optimistic or pessimistic about the future?

Dr Grabosky—I think I am a born optimist, just in general terms, so I am fairly optimistic about the future. I think that those with significant assets to protect are increasingly becoming aware that their future security and prosperity will depend upon their ability to access and implement state of the art information security technologies, and they are doing that. I think this is a very challenging time for law enforcement in that, as I hinted at not long ago, the nature of policing and of police organisations is in a period of revolution. I was thinking not long ago about how basic critical infrastructure—electric power, telecommunications and so on—in most of the industrialised world now exists in private hands, rather than under state auspices, and this is a very significant challenge for those who would protect the national infrastructure against malicious attack. This has necessitated the creation of new organisational forms to achieve that, new ways of effecting communications between disparate institutions.

Technology is a double-edged sword and all technologies have had upside and downside potentials. I think that information technology, for all the risks that it poses, is providing enormous benefits in so many areas—education, communications, commerce and so on—that I cannot help but feel optimistic.

Mr EDWARDS—I have concerns about many issues related to law and order, and particularly with regard in our country to the suspicion of one police force being less than honest in its actions—in other words, negativities about particular police forces in this country from other police forces. Do you think that governments should be more lateral in their thinking, other than the traditional law and order response? Is anything less than the coordination of a national response to cross-border crime likely to fail?

Dr Grabosky—I think that, given our federal system, Australian governments have taken constructive steps towards overcoming the problems that would traditionally flow from a system involving multiple jurisdictions. About a year ago the conference of police commissioners met here in Canberra and established the working party—with which I am sure you are familiar—that produced the scoping paper under the auspices of the ACPR. The efforts on the part of ACPR to establish a national community of forensic computing investigators in the various police services of Australasia I think are quite commendable. I cannot emphasise more, however, that the world does not end at our shores and the imperative of international cooperation is going to intensify. There are still anomalies in various laws that I think provide certain criminal opportunities and authorities in each of the relevant jurisdictions would be well advised to identify these and to rectify them.

Mr EDWARDS—Finally, just referring back to the issue of privacy, as a member of parliament—and, more specifically, as one who has an interest in the issue of the distribution of drugs in this country—I was alarmed to learn, in my capacity as a member of another committee, that cameras which are used as an implement to keep drug distributors and users off the streets in some of our cities and which film drug transactions are, because of the privacy issue, not allowed to be used as a tool on the individuals that are filmed by those cameras. In fact, the input from the police into them is that they are able to view them and then the cameras are retained by the local government body that has installed them for a period of a number of days and then destroyed. I find that reprehensible in terms of that tool being used to do something more constructive in terms of addressing the distribution of drugs in this country. Would you like to make any comments on that?

Dr Grabosky—I cannot comment authoritatively on the law relating to the use in public places of video surveillance, except to say that it is used extensively in the United Kingdom and I think it has received increasing attention here in Australia. The potential for detecting criminal activity and identifying suspects is, I think, self-evident. The question remains as to how these technologies are deployed and what use is made of them. Whilst there are some privacy considerations to be undertaken, one again would want to balance the interests of the individual against the interests of society.

Mr EDWARDS—Thank you very much.

CHAIR—As you will have gathered, we probably have a reasonable understanding of some of the questions and we are looking for some potential answers. I wondered whether, Dr Grabosky or Dr Urbas, you are familiar at all with the UK's Regulation of Investigatory Powers Act 2000?

Dr Grabosky—I am afraid not.

CHAIR—We wondered if that might be a model but if you are not familiar with it then there is no point going down that route. Can I thank you both for coming to talk to us this morning and giving us the benefit of your expertise and information. Thank you very much indeed.

Proceedings suspended from 10.39 a.m. to 10.55 a.m.

DURIE, Mr Robert George, Executive Director, Australian Information Industry Association

LARSEN, Ms Bridget Anne, Legal and e-Policy Manager, Australian Information Industry Association

RANKIN, Mr Murray Grant, Representative, Australian Information Industry Association

CHAIR—I now welcome the representatives of the Australian Information Industry Association. The committee prefers all evidence to be given in public but you may at any time request that your evidence, part of your evidence, or answers to specific questions be given in camera and the committee will give consideration to such a request. We have received your submission, which has been published, and we have also published the submission from Mr Rankin in his capacity as managing director of The Distillery Pty Ltd. Would you like to make any opening comments before we go to questions?

Mr Durie—Thank you, yes, just very briefly. I will not go over any of the issues in the submission but I will mention two things which we did not cover in our submission. The first is on the issue of skills, and I think the committee will be aware of the general shortage of IT skills in the community. The data we have shows about 30,000 jobs cannot be filled. We think that the position of the law enforcement agencies in attracting suitably qualified skilled people in the IT and cybercrime area is going to be particularly difficult and one of the resource issues that the government is going to have to pay special attention to. The cost of people with these skills is being bid up considerably by the industry, and there is a shortage in any event. I think that is an issue that will need to be addressed.

The second point I wanted to make was to advise the committee of some work that AIIA has been involved in internationally. One of the themes in our submission was the importance of industry and government cooperation on cybercrime. AIIA participates in a number of international organisations of like kind. One of those bodies, the International Information Industry Congress, last September finalised—and I think since we did our submission has released—a position paper on cybercrime which covers a range of issues which are of interest to this committee. We will provide a copy of that paper to the committee as soon as possible.

CHAIR—Thank you. Just taking up your point about the problem of enough skilled people and the difficulty that government bodies suffer in terms of competitive salaries compared with others, I think that is a problem that the committee had already understood. I suppose my question is: do you have any sensible suggestions for how that could be addressed?

Mr Durie—I think it is part of the overall issue of IT skills, and there are no simple or immediate solutions. For example, if you look at the government's initiative in backing Australia's ability to provide 2,000 additional places in ICT, maths and science, it is very welcome, but the problems are the universities do not have the infrastructure, the teachers et cetera, to actually take up 2,000 places. They already cannot fill the places they have because of a shortage of teachers. Secondly, it is going to take four or five years for those people to come

out the other end of the system. So you need to take a holistic approach. The government is doing some things on immigration which are useful but there needs to be much more attention to, as I say, a holistic approach to making sure that the whole system is producing more people with skills. I think it is also an area where government/industry partnerships might be able to help, both in terms of assisting the infrastructure in the education system and also more directly assisting working with law enforcement agencies.

CHAIR—You are the industry experts. Apart from the Internet, what other newer forms of technology are coming through that we should be aware of?

Mr Durie—I am a generalist so I will take the liberty of deferring on that question to our industry expert.

CHAIR—You may pass the ball to either of your colleagues.

Mr Rankin—I will speak from the law enforcement capacity in that regard. The challenges of technology, I think, are going to lie not so much in what is coming down the track, because I think there is a great debate in academia about post-Internet technology, where is that taking us, the whole e-commerce revolution and the specific fields within that business-to-business, business-to-government, government-to-government type of exchange. I think the thing that needs to be emphasised more than anything is law enforcement's ability to actually uptake that technology and keep pace with the change of that technology, which I think re-emphasises what Rob said earlier about that skill shortage being exacerbated by the brain drain from law enforcement, and from government in general, across to the private sector. I think that just exacerbates the problem so that law enforcement has trouble meeting that challenge of what is to come in a number of capacities.

It is always the futurist's vision to say what is around the corner. I do not want to get into the technical specifics but I think the challenge lies within the Internet domain and where specific technologies are developing that law enforcement needs to understand. For example, this big push on business-to-business and government-to-business transactions is going to be an increasing area for cybercrime in the area of fraudulent transactions and, if you want to look at it like that, the passing of either data or financial information across international boundaries is an area that I think will be a big growth area.

CHAIR—So, with regard to the people who will be involved from a crime detection point of view, do they actually need to be technologists or do they just need to understand how the technology might operate?

Mr Rankin—I think a combination of both. I think that the answer in that lies in recognising the challenge in the core competency. The question should be: should law enforcement be technology experts or should they be law enforcement experts? As such, possibly the answer lies in closer alignment between government and industry that can stem some of the issues with that brain drain—so cooperative syndicated relationships with subject matter experts. I think there will always be an element of expertise needed by law enforcement because of such issues as the evidentiary nature of the information they are dealing with and the admissibility of it, but I still think that can be dealt with from the private sector, being subject matter experts, assisting law enforcement in that capacity.

CHAIR—You mentioned earlier on that you were going to give us a document about the international conference. What is happening overseas to deal with some of these issues, because obviously Australia is not alone?

Mr Durie—I do not think there are any simple solutions anywhere. In fact, looking at the recommendations of the paper about what needs to be done, it is really addressing the same issues: how does government get the resources it needs, the issue of producing more graduates with relevant skills, more training inside law enforcement agencies et cetera. I think everybody is grappling with the same issues.

CHAIR—Just setting to one side for a moment the fact that the people with the right skills are in short supply, whether they are in the private sector or the public sector, there are other relevant issues to crimes using the new technologies that are now becoming available apart from just having the skills to deal with it. Even if you have the skills, there are a lot of other questions about access to the technology, whether there should be prohibitions on certain technologies being allowed in the public domain, how you actually fight the abuse of some of those technologies, the privacy issues that might be associated with it and so on and so forth. Has your organisation done any work in that area?

Ms Larsen—There are a lot of other avenues that might also be used to address this issue, and one of the things I think is important is educating consumers who have access to these tools about what the tools can do, what the risks are and what measures they can take—whether they be technologically or just in the way that they interact with those tools—about the dangers and preventing vulnerabilities.

You mentioned about banning certain technologies. I think that is something that is being discussed in Europe particularly. Our view on that is that the technology itself is not causing the harm; it is the way the technology is used. So, rather than banning hacking tools, for instance, which are very valuable in assessing security vulnerabilities, it would be better to put guards around the use of those, or in the legislative sense say that they can be used for purposes which are legitimate but not other purposes which may not be legitimate. I think that is something that is being reflected, for instance, in the digital agenda legislation.

CHAIR—Do we have the technical ability to say regarding hacking tools, 'They can be used in this context but not in that context'? The police might want to have some hacking skills available but we clearly do not want the average citizen hacking into the government's defence secrets or the banks or whatever. How do you control it? If the tools are out there, how do you control it? How do you know what is a legitimate use and what is not a legitimate use? How do you define that?

Ms Larsen—It is the same as using an axe. You can use it for good and bad purposes, and you will not know until it is used. It is going to be a matter of community education about when it is right and when it is not right.

CHAIR—If I cleave one of my colleagues' skull with an axe, the evidence is very obvious there; it is not difficult to detect. My question is: using these technology tools, how do you detect them?

Mr Rankin—I think the answer to that stems back to the original question. One step of that is: how do you detect it? I think 'technology' is the answer, but maybe the question lies in who detects it. Is it law enforcement's job to do the detection or is it law enforcement's job to enforce the law in that capacity? I think the pragmatic approach to this type of problem, once again without harping on that point, comes back to identifying those subject matter experts as areas of core competencies and allowing them to deal with it. I think there are examples in both the government and private sectors where there is adequate expertise in those areas, but I do not think there is enough being done about cooperative collaborative approaches to dealing with that problem.

CHAIR—That is one of the reasons why we are asking industry to give us its views on some of these issues. In talking to a previous witness my colleague gave the example of infra-red tools that people could use to scan private houses, whether they wanted just to observe the occupants' individual peccadilloes or whether they wanted to see whether somebody was in the house before they broke in to rob it. Does the industry have a view on the use of technology and the unfettered use and distribution of technology across the community?

Mr Durie—I think from a level of high principle we would be opposed to blanket bans on particular technologies on the basis, as Bridget was saying earlier, that all of these technologies were designed originally to be used for good and do have positive applications.

Mr KERR—Isn't that a bit like the argument that guns don't kill people? I am troubled by the libertarian sort of position that is often asserted by the industry that all these things are fine provided you tell people that they should not do bad things and that that is where you should draw the line. We know really that the capacity for law enforcement is virtually zero in some of these areas and there is no private consumer capacity to address these matters. Maybe some of the large companies can do a bit of self-help, but even there I think there is some significant doubt as to their awareness of the degree to which they are at risk. I am just wondering whether that is a particularly naive position to assert to us in terms of a public position.

Mr Durie—Sorry, I was halfway through my comment, and that was the matter of high principle—

Mr KERR—I am sorry, that is just a rude member of parliament taking over.

Mr Durie—No, not at all.

CHAIR—He is from Tasmania and we make allowances.

Mr Durie—I am not sure how I should answer a question which is inviting me to identify myself as naive. I think as a starting point we would not want blanket bans on technologies, but I take the point that, as with guns, there are going to be areas where with experience you will want to decide to either ban or place controls on their sale or use, but I would have thought that is going to be very difficult. I am not sure that parliament would want to be leaping into that without having considerable evidence that that was desirable and was going to be effective, and I certainly would not want it to be the starting point. But I can see that there are circumstances—for example, gun control laws and radar detection devices et cetera—where we already do have controls of some description on technology, if you like.

Mr SCHULTZ—Just looking at paragraph 413, which is headed as 'Enforcement Authority', some of the issues raised in that paragraph centre around the need for government agencies to work with private enterprise, which I virtually do not have any problems with. But it brings to mind to me that part of the problem with governments today is that you have, as an example, very capable police officers working in the various police jurisdictions that are capable of being upskilled, if that is the word, into the IT area and there is a haemorrhaging of a certain percentage of those people into private enterprise. I take on board the comments that you are making with regard to those people having access to the equipment they need to assist them, but also would you see private enterprise, rather than poaching those sorts of individuals out of the law enforcement area, as working with the law enforcement area to help upgrade their skills? Do you think that governments have an obligation in terms of getting their workforce up to the levels of skill that are needed and, because of the rapid increase in IT technology, remunerating officers to the extent where they are retaining them within the service rather than losing them out of the service?

I suppose it is a pretty broad question I am asking. I have a personal concern about the good people that law enforcement areas are losing to private enterprise because it has a backfiring effect in terms of our ability to address the crime issues that we need to be addressing because of the skills that we have lost within our enforcement agencies.

Mr Durie—I do not think there is a simple answer but, absolutely, the government should be putting more effort into training its people and raising the skill level. I think there are certainly opportunities for the industry to help with that process, and also too, if you like, to have perhaps closer links in terms of skill development and skill transfer. At the general level, the industry has already established a body called the IT&T Skills Exchange which is looking at developing, if you like, transition courses—I hate that word 'upskilling' but we seem to be stuck with it—for people who want to stay in their discipline but have a better understanding of IT. So the industry is actually putting some of that in place. One of the areas that have been identified as being in high demand is security, so that will have some benefits.

In terms of remuneration, obviously as an employer the government has to respond to some degree to market movements in salaries. We do a quite substantial remuneration survey for our members, which gives guidance on salary movements. I think the headline number over the last 12 months is, on average, something around 10 per cent, but that includes office workers in the industry. If you look at the skills in demand, you are probably getting movements more like 15-20 per cent in salary. It always makes me realise that I made a very poor career choice not being an IT professional, but never mind.

CHAIR—If it makes you feel better, I used to be an IT professional -

Mr Durie—Yes, I am aware of that.

CHAIR—And I can assure you that you are a lot better paid now that I am.

Mr Durie—I recall that you were the Canberra manager of one of our members at one point.

CHAIR—That is right.

Mr Durie—The point I was going to make was, yes, remuneration is important, but it is not the only issue. One of the things the government might want to look at in this is: what are those broader elements of job satisfaction that keep people with IT skills engaged and interested? For example, not every IT professional in Australia has rushed off to Silicon Valley where you can get paid 40, 50, 100 per cent more than you can get paid in Australia. There are other elements which keep people interested. I suppose my view would be that the more effort the government puts into actually coming to grips with the issues in IT security, the more it is going to be able to provide very interesting jobs for professionals, and they are actually enthralled by these technical issues.

Mr EDWARDS—So you are effectively saying that, given those circumstances, job satisfaction will keep those people there?

Mr Durie—It is not going to keep everyone but job satisfaction goes way beyond money.

CHAIR—What would your view be of either acknowledging that each law enforcement agency of one sort or another around the country has a need for this IT expertise—or technology expertise is probably a better phrase because it is more than just IT—given the difficulties of recruiting and retaining, or whether it would actually be better to have a single agency that provided the technology expertise across the board for law enforcement agencies? That way you would actually have, perhaps, a large pool; you could make special employment conditions, perhaps, and retain those people, given their interest in the actual nature of the work. When people come to the end of a particular project or issue and there is no further development—if they were working for the Western Australian police, for argument's sake—they would say, 'There's nothing much interesting here; I'll move on.' But if they were in some central body they might then find there is an interesting project in some other area. I am not expressing a view one way or the other, because clearly there is the need for specialist knowledge within each sector perhaps, but do you have some views on whether big is beautiful in this instance or distribution is the go?

Mr Durie—I would not want to leap into giving advice to the government about the structure of law enforcement agencies, but there is an attraction, if you like, without bringing the agencies together—and I cannot really comment on whether that is desirable or not—to creating something, in the same way that you do, for example, in the Commonwealth public service. There is tremendous mobility between agencies of people with IT skills. So you might be able to have an informal or whatever degree of arrangement between law enforcement agencies which create a common approach to skill definition, increased mobility et cetera so, without merging, they pool their skills in a way where they could allow people to move from one agency to the other when there are projects to be done.

CHAIR—Are you familiar with AUSTRAC?

Mr Durie—Yes.

CHAIR—It seems to me that AUSTRAC is a special agency. Obviously its work has an interest to a number of different law enforcement agencies, but it needs particular skills and salaries and so on and was set up as an independent body as such, or a separate body. I am

wondering whether that might be a model for doing something similar on a broader technology front? I am interested in the industry's view.

Mr Rankin—I would like to add that I think one of the challenges facing government when it looks at that type of solution—which is another agency or a shared agency or superagency – is that it has to take a step back and look at some of the issues that that same agency would face that the current law enforcement agencies face, and Rob mentioned a few of those in terms of the mitigating circumstances, such as remuneration and the other factors that are the pull factors out of the public service into the private sector. One of the big problems that has been my experience in my former law enforcement life has been that the government in a lot of ways is encumbered—not withstanding due process—in technology uptake et cetera, so in a lot of cases that whole innovative drive, the whole entrepreneurial drive, that fosters the business community is non-existent, or exists to a lesser degree, within law enforcement, and hence they are the major pulls that are attracting people away, albeit that they happen to be attracting them with big dollars.

But, as Rob says, I do not think that everyone is dollar motivated. They are innovation, quality of life, job satisfaction motivated. I think there stands the challenge for a common agency. I am sure AUSTRAC does a great job in its expertise, but I am pretty sure from empirical evidence that it suffers the same problems of expertise being drawn away, and particularly in an industry that can probably well afford to in that regard. I think there lies the challenge to that type of approach.

You mentioned earlier about prohibition et cetera of certain things. From a public policy point of view, that type of approach needs to take a look at the cultural shift that the Internet is causing within society. We have had examples in the past—predominantly from the States across to Australia—where for such things as encryption keys et cetera there has been an attempt, for appropriate reasons, at control. However, the pervasiveness of the Internet simply means that people have the means to distribute that to countries that are not parties to signatory agreements et cetera, and it means that that technology is now available in the public domain. I think the cultural shift in the way society will operate in the future, because of this whole e-commerce Internet-driven society, offers new challenges to public policy. A very good example is about the infra-red camera, for example, with people planning to break into houses. I think in that particular case the questions will be: is that technology going to be able to be banned and is it cheap enough and simple enough to build in the future? They are the challenges, I think—those cultural shift changes.

I think the Internet has substantially changed the playing field so that a lot of traditional responses in the past—I do not really have any great answers for what they are in the future, other than recognising that I think there is a significant shift and public policy needs to deal with that shift—

CHAIR—I think we agree with you. Fundamentally, that is why we are holding the inquiry, because we are trying to look for some suggestions as to how we might put forward some recommendations to start to shape some of that public policy.

Mr SCHULTZ—I would just like to follow on from the comments that I made to Mr Durie. Mr Rankin, I notice on page 3 of your submission you refer to the issue of cybercrime and how

the AFP have emphasised that it is one of the greatest problems facing law enforcement. I am absolutely amazed and I find it reprehensible in the extreme that—despite an offer made by you to assist them in that area, in an environment where you say the chair of Conference of Police Commissioners of Australasia, Mick Palmer, was quoted as emphasising that 'a key element of the strategy will be developing partnerships with a range of stakeholders, including the private sector, which would look to resource sharing and enhanced cooperation with these groups'—you are offering that sort of expertise to the police forces of this country and they have not even bothered to acknowledge that offer or indicate a keenness to participate in that sort of assistance. Is it any wonder that we are going down the track that we are going down? Would you like to comment on that?

Mr Rankin—Yes, I will. I suppose the comment should come from Murray Rankin, The Distillery, and not as a representative of AIIA when I say this.

Mr SCHULTZ—Sure.

Mr Rankin—Firstly, I do not know what the due process is in the deliberations to respond to offers made, but I think one glaring example of the whole flavour of what we have been saying this morning is that a very senior member of that committee that was set up was ultimately poached across to the private sector and hence the whole ramifications of what we have been talking about become a living example of the whole problem. I do agree that we were at a loss to explain why the offer was not taken up further, but I reiterate that I do not understand the processes for selection and deliberation. There was a public offer broadcast in the public domain for businesses such as ourselves in the private sector that may offer. I do not know what response there was or what the quality of those responses were; maybe we were cold et cetera. I do not know what the answer to that is. Certainly, from the private sector point of view, it did surprise us as well because we believe, as I am sure many of our peers in the private sector would also believe, that we have a fair contribution to make, both on a technology basis and a former law enforcement basis. So, yes, I agree.

Mr SCHULTZ—Quite rightly so. Thank you.

Mr KERR—I was interested in this intersection between the nation and private enterprise. Firstly, there are some large structural vulnerabilities that I suppose you put into the security basket, and one of the responses that the government has made is establishing the National Information Infrastructure Taskforce. I have had the advantage of talking to some people involved in that who have not been particularly flattering in relation to the way it operates. I would appreciate some comment about that and whether there should be some revision of its approach and perhaps a greater integration. Perhaps you could respond to that and then I might follow that up. Are you aware of that as a concern or an issue?

Mr Rankin—I may defer to Bridget in terms of the national infrastructure issues because I believe she has—

Mr Durie—She is actually on the subcommittee.

Ms Larsen—We are involved in the National Information Infrastructure Consultative Industry Forum and have been participating in that more actively over the last year. We agree

that the two issues that they are focusing on, incident reporting and security awareness, are very important. We are participating in the working group on security awareness and have helped finalise the RFT for the business plan, so we are working quite closely with them there. I was pleased to see that it seems to be that they are refocusing their attention on the issue and elevating it, and certainly we have had more fruitful discussions with representatives of the National Office for the Information Economy just in the shorter term. The Industry Association is very keen on these issues.

We are running it through what we call our e-Policy Taskforce and what we are going to be doing is pulling together the industry position on each of those issues and presenting that to the consultative industry forum, as well as using it directly in consultations with NOIE. They issued yesterday, I think, a work plan identifying a number of key issues. We had some input into that and I think that they are the right issues to pursue.

Mr Durie—Having said that, it is moving with glacial speed. This group has been around for two to three years and it has had various characterisations. I think NOIE, the National Office for the Information Economy, is now more involved—

Mr KERR—There was a shift of where it is centred, was there not?

Mr Durie—Yes, it used to be in Attorney-General's but I think now it is across with NOIE. It remains to be seen whether the pace will pick up, but obviously the issues are moving pretty quickly and the response is certainly not keeping pace.

Ms Larsen—It has the potential to do a lot of really good work. They have the right sort of players around the table from an industry perspective but there has been a lot of frustration about the rate of progress. I think one of the reasons is that it has tried to be too many things to too many people. There are people who are interested in the policy development side, there are people involved in the more day-to-day technological aspects, and a group of that size cannot address all of those interests.

Mr Durie—Just to finish up on that, there is a neat link between our input into that work and the participation we have in the global work that the industry is doing on information security where we formed, with our counterparts—and in the group there are 45 national IT associations involved—a working party specifically to look at information security. We held a global conference on information security in Washington last October. Unfortunately, we were not able to get any Australian government participation in that. There is another conference happening in Belfast in late May. The whole purpose of these groups is to bring together industry and government to form, if you like, a global alliance to look at these issues, determine priorities and actually get some work done. We would certainly be very keen to have the government participate in that process more—they cannot participate any less, put it that way.

Mr KERR—That largely reflects the sorts of reports I have had as I have travelled around. In traditional policing, the model is that the citizen is expected to play some role in their own self-protection—for example, we encourage people to lock their cars, put deadlocks on their houses and to be careful with their personal safety—but when an incident does occur we do not expect the individual to pursue the investigation or enforcement of the law. That paradigm seems to be challenged in this area because, if I am correct, there are something in the order of 12 people in

the cybercrime area of the AFP in core competency. That works out to about one per one million of the adult members of the Australian community and probably gives them, if you look at a sort of a simple division, about seven seconds per adult in their working day to reflect on and address what might be a very large issue.

That has meant, of course, that routinely the AFP refuses to investigate matters in the copyright field and in a whole range of fraud and what have you, which most of us would say are pretty serious crimes. I suppose in those circumstances they could hardly do any other; they have to prioritise their responses, as does the National Crime Authority. But that means then that law enforcement has to be transferred across to the private sector and that leads me to a fairly worrying new paradigm of where the citizen stands in relation to a growing burgeoning of private law enforcement. There are now, just in the physical law enforcement environment, more people in private detection agencies and private security than there are in all law enforcement agencies in Australia, and immeasurably more so in the cyber environment.

That is a very substantial shift in a very short period of time and it means that essentially even one of the basic functions that we used to confer on the state, a reliance on security as an ultimate guarantee of citizenship, is now being shifted across to the private sector. That is fine if you are a big corporation but not so fine if you are a little guy because you do not have the resources to be able to step in and fill the void. I just wonder if you have reflected about these kinds of issues, because they are starting to be very significant in my mind as one of the biggest challenges to the kind of society that we will be growing into. All of these things occur incrementally, but very fast; our social responses occur incrementally, but, as I think you said of the Attorney's Department, sometimes glacially. So the gulf between what is happening on the ground and the social response gets wider and sometimes we really do not know what is happening until great social transformations have occurred. I just wondered whether you have any comment about this. You are, presumably, right at the cutting edge of requests for law enforcement responses, but of course you would be aware that if you are a small individual or a small corporation there is just nowhere to turn at the moment.

Mr Durie—If I could start on the copyright issue, which obviously is of great importance to our industry, particularly the software sector. It has been, if you like, a bone of contention for the industry that they have had to undertake their own enforcement. A group originally formed in the United States many years ago has been here for about 10 or 11 years called the Business Software Association of Australia. That is the group which actually 'enforces' copyright law in relation to software in terms of illegal copying, piracy and so on. It is essentially made up of the large US software vendors—there are a small number of Australian vendors involved as well. They do not have 11 people dealing with it; I think they have one investigator and another person manning a hotline, and may just focus at the very big end of town. So their goal is to trap, if you like, to gather evidence about major corporations, large resellers et cetera, who are breaching copyright provisions and then bring that to the attention of the AFP in the interests of launching an investigation. I am not a lawyer, but I think there are some circumstances, Anton Pillar orders and whatnot, to—

Mr KERR—They can pursue their own remedies.

Mr Durie—Yes, and they take them to court et cetera. That is the tip of the iceberg because, if you think about pirateable software, there are only a relatively limited number of companies

now, given the rationalisation in the sector, selling those sorts of products. They are readily identified: if you can actually look at somebody's PC you can readily identify whether they have these software packages on them. If you turn then to cybercrime, everyone is involved. Detection is way harder than working out whether you have a copy of Word or Outlook or whatever on your PC. I think we have not started down that route—certainly the IT industry has not—although I imagine that a lot of detection work goes on in and around, for example, data processing centres and the like, web sites, and we have all heard of the examples of Microsoft, Yahoo, Amazon et cetera, being brought down in the last six months. Presumably they are doing a lot of work, firstly, to prevent those sorts of incidents and, secondly, finding out who the hell it was who was doing it. But there has not been a concerted response on the part of the industry to deal with that to date.

Mr KERR—All of which is true, but all of those corporations have economies which if you compared them would be larger than those of most small nations. They can afford to have a network of sophisticated monitoring and detection, although when I have had discussions with people in the United States and here who look at this NII issue they do point out that even many large corporations are greatly unaware of the degree to which they may be the subject of vulnerability.

Mr Durie—And particularly outside the IT sector, I would have thought.

Mr KERR—Yes, exactly. But, notionally at least, a corporation the size of Ford or an electricity generator which might be the subject of attack would have the financial resources, were it to see it in its interests, to accommodate some protection. But this leaves unprotected the vast majority of us as private individuals and small corporations. So the traditional paradigm of policing is not working; there is no private sector paradigm that could exist, presumably, in this vacuum. I am just wondering how we start to address this. It is a big step down from the National Crime Authority in some ways, because in one way that is the equivalent of the top end of town because its focus is on organised crime, usually with an interjurisdictional nature. But, to the extent that that impacts to any degree on me as an individual, were I to be a small publisher and find the titles that I am publishing being electronically transmitted and sold without my consent—were I to be impacted in a whole range of ways—it is frankly beyond anyone's capacity to step in at the moment. The AFP routinely refuses to investigate even the big ones.

Mr Durie—We actually had this discussion while we were having a cup of coffee before we came over—that there is nobody to call when this sort of thing has happened. I will ask Murray to comment in a minute, but I think one of the answers is about education. If you take sort of a narrow slice of what we are talking about as, say, viruses, you can do a lot in terms of protection if you understand what you can do in terms of anti-virus software—

Mr KERR—I have a 12 year old who might, but hang on.

Mr Durie—That is right. Unfortunately, we need to get across that, even the oldest of us, because it is going to be critical to our businesses—think of what has been happening in the last couple of months with various viruses that have been going around. If I can just talk about AIIA's experience as a small business which does not have an internal IT function. Despite our membership, we do it ourselves if you like, out of our own resources. Because of what we

know, we have made protecting ourselves against viruses a priority for the business and we have not had any issues when these viruses have swamped the world. Anyway, that is me from a generalist point of view answering. I think Murray probably has some more technological comments.

Mr Rankin—I think one of the big issues to fully understand and explore is this whole issue of what is cybercrime, and I think it is well overdue at a holistic approach to deal with this. Traditionally you can look at cybercrime basically being broken into three areas. Firstly, you have your technology-type crime, your hacking et cetera, which does pose a real threat to issues such as the NII and large corporations and government's capability to do its business. Secondly, you then have the traditional crime that is being committed in a new medium—criminals are basically opportunists and they all of a sudden find that the same scam they could run down on the corner they can now run anonymously on email or whatever.

Mr KERR—The Nigerian fraud letters.

Mr Rankin—Exactly, yes, and fly-by-night organisations where the Internet allows them to put up a front and you think you are dealing with a reputable organisation and you are not, things like that. Then you have your third element, which is the new crime that may not even exist yet that the new medium gives you opportunity to do, such as interception of data and changing the data en route and then it arrives at its destination and it goes into someone else's account, or something like that, those type of things. One of the areas that I think we need to fully explore and understand is the trade-off between the focus that goes into those areas. For example, at the NII level, in equivalent law enforcement examples you have adequate response by the public sector in the areas of SACPAV and counter-terrorist type large emergency management type thing, which is a coordinated approach by Commonwealth and the states. I think that type of approach to the large NII type issues is the typical sort of approach you need. You need a coordinated approach drawing upon the resources that are at the disposal of the country to combat that issue.

But then when you start looking down at some of the more traditional ones it becomes a law enforcement response to say, 'How do you want to separate a detection or prevention-type approach to the traditional crime in a new medium and the new crimes that we may not have the skills to detect and deal with?' I think if we approach it pragmatically and break it down into those areas and any subsets that might come out of that it gives us a way forward to deal with it in that capacity. We have to be very careful, as an industry—and particularly from a public policy point of view—not to create a monster out of this thing called cybercrime. We have examples where we try to control things traditionally that are outside the country's general control—for example, we have customs and immigration type controls for goods and services and people across country boundaries. Under e-commerce and globalisation a lot of those disappear in the data environment so we need to address ways that we can apply a similar sort of model to that.

As soon as you raise that, you are going to start coming up against the big brother type mentality, the trade-off between how effective you can be at detecting and preventing that and also making sure that you do not stifle economic growth, because the whole point is that governments need to trade and businesses need to trade and we cannot put too much of a bureaucracy over that. To wrap up what I am saying, I think the approach can be a pragmatic

one. The US, for example, recognises this fact and has cyber teams set up within the FBI. In their strikeforces they have cyber teams set up within the customs service—customs being responsible for any activity across a US border, and particularly in cyberspace. So there are examples. I do not know about the NII-type response at other country levels but we certainly have models in place in Australia that adequately deal with the threat outside a technology model. Maybe the answer lies in exploring those on a more pragmatic basis and not getting too caught up in the fact that this is high tech, but to fully understand what is high tech about it and address those issues.

Mr KERR—I am curious at the small end, again coming back to the ordinary citizen or small business. It is frequently said that the most common mode of communication that people use in the electronic environment, which is email, is insecure. Can you just tell us why it is alleged to be insecure and what are the self-help mechanisms that people should use? You can use pretty good privacy, I suppose, but that is a nuisance at each end, is it not?

Mr Rankin—I think it is. Without dwelling on technical specifics, there are mechanisms to ensure the security of transmission: data encryption, trusted services. The two elements of security that the government is doing a good deal of work in are not only to ensure that the means of communicating is secure but also that there can be a certain level of confidence and quality assurance that what goes across those secure lines arrives as intended at its destination. From the small end of business, there are plenty of commercial products available that meet that level of security. I think it comes back to what Rob and Bridget were saying earlier, that one of the key elements is education, and it does not need to be under the heading of cybercrime or a high tech response. It is no different to how you would normally operate in a modern society in terms of health, in terms of your control and protection of your own personal assets—for example, you do not go and give your credit card around to everybody—and you should be aware of things like when you start to deal in that area.

Mr KERR—Just treat me as very ignorant, but what should I assume when I send a personal email transmission, or a small businessman sends one? Should I assume that it is an open network that anyone can intercept or should I assume it could be intercepted by a hacker if they can get in to my system somehow? There is a real level of paranoia emerging, and I use that word advisedly because I have had so many reports from people who believe that their email has been read by people. They usually believe it has been read by state institutions and I dismiss that because the requirements for state institutions to bother about that level of transmission is very slight, and they would need a warrant and the risk in proceeding without one is too great for them to undertake. Are these open transmissions that are easy to intercept or are they hard to intercept? What is the normal level of satisfaction I can tell people when they make these complaints to me?

Mr Rankin—I will answer that question in two ways. I think that pragmatically it is a 'buyer beware' type attitude. It is no different to how you would treat sending something on a facsimile or sending something through the post in terms of that. There is certain legislation in place to protect those types of transmission, such as letters in the post et cetera—as you say, there is the Telecommunication Act and they are protected in such ways that you need warrants et cetera to intercept that traffic. I think the issue once again is a pragmatic education principle: be aware that just as a conversation across the back fence is no more secure than you think it is because

there is only you and the other person there. So I think that one approach to it is a 'user beware' type—

Mr KERR—Really treat me as an idiot here. When I am talking over the back fence I can sort of think that I am so far away and, yes, there could be somebody with one of these hearing devices pointing it down and scanning me but essentially you can have a look around and see whether somebody is there and in the normal course you can say that that is a secure conversation. When I send my letter on the email saying, 'Please meet me at such and such for a cup of coffee,' can I assume that on all but a rare occasion that is a secure transmission, or can I assume that anybody who wants to can read it?

Mr Rankin—Unless you are using a type of encryption algorithm or tools that ensure that privacy, you would say that it is an insecure transmission, simply because of the nature of the networks that are going across. If you are using the public network, such as the Internet or something like that, you cannot guarantee how many mail computers that email is going to go through—it could be hundreds, depending on where you are sending it to—and you have no idea where that is going en route. Secondly, you have no capability to deal with the scruples of people who may have access to that. The thing that balances that is that if you are looking at typically an Internet service provider which is offering that facility—and there might be hundreds of them in the loop to get from point to point on that email—you also have to deal with the pragmatics of the fact that they may be receiving hundreds of thousands, even millions, of emails. It gets down to the trade-off about the value of going to that effort to read that mail. I am not saying that should be ignored; it is a very real thing, but it really comes down to an economic trade-off: I need to find that and then what value am I going to get from reading it, and of course, do I highly value that?

I think one of the value-added services that businesses are now offering to the community as an incentive to do business with them is that they will guarantee a certain degree of, if not guarantee, privacy across that network. So, from an individual's point of view—and I know we are talking down the low end of the problem here—in a normal sense if you are not using security and encryption technology, which is commercially available and relatively inexpensive, then you have to assume that the message in the email and the attachments that may go with it are insecure.

Mr EDWARDS—You are aware, of course, of the Australian Bureau of Criminal Intelligence's database, ACID. Why do you consider that your own product, InterQuest, is superior to ACID? How do you overcome the commercial advantage that you see the ABCI has?

Mr Rankin—On the first part of the question, why do I think it is a superior product, a large proportion of employees within The Distillery at the moment are ex-law enforcement people who worked directly or indirectly in the past on systems such as ACID and other systems. One of the frustrations that we have dealt with today has been the impediment that exists within the public sector for creativity and innovation, and in a lot of cases rightly put in place because you are trying to deal within a budgetary constrained environment or to meet a specific set of agency requirements or whatever. The initial systems, such as ACID, were constrained by those impediments. There were innovative opportunities that were either not seen, not taken up et cetera, and that led to opportunities in the community sector outside. So I am in a position to

say that, based on the technology developments that have happened in the private sector, products such as InterQuest are superior to other technology that exists in law enforcement—such as ACID and other systems—simply because I have knowledge of both systems.

Why does that environment exist and how do we combat that competitive environment? It exists because ACBI, as one example—and there are many examples of this in this case—offer a service under their charter, which they are fully entitled to do, but by the nature of the business they do not operate on the same economic playing field that private sector organisations, and maybe some public sector organisations, are forced to play on. Hence, a lot of the potential users of private sector products take the decision to use what would arguably be inferior products because of things such as budget constraints and the price of that service. They are prepared to accept a lesser service at a cheaper cost because of agency constraints. When a private sector company tries to deal with those issues on a commercial transaction basis it is a very hard argument to counter, 'Why should we pay X for a commercial product when maybe we're willing to live with some of the deficiencies but at next to no cost?' or a free service in some cases.

While ever that monopolistic attitude exists within the public sector, the nature of those human decisions naturally means that they are not going to get access to the best technology that is available. It comes back to the original discussions earlier about why doesn't that innovation exist. It is because the public sector, albeit having budgets et cetera apportioned to them, do not have to operate on the same economic basis as private sector industries—they do not have to make sure that there is revenue and cash flow to keep salaries paid and people employed. Therefore, the private sector business is continually being forced to look at innovative ways to sustain that competitive advantage. In a lot of cases that is directly attributed to meeting client requirements—they may have an issue they want solved or something—but while ever that innovation and competitive push is non-existent in the public sector, I do not think they get the best technology that is available.

That has been recognised by other overseas agencies. The director of the FBI, Louis Freeh, has recently said that they cannot keep up internally with the pace of technological development. Also, the CIA has gone to the extent that they have set up a cooperative Silicon Valley venture capital firm to invest in high tech companies to assist in them playing the catch-up game because they felt they had fallen behind in the necessarily secret world of intelligence operations. I think that is exactly the answer to that question.

CHAIR—In the introduction and the last paragraph of your submission, Mr Durie, you say that you have only made general comments in your submission and did not intend to address the more detailed issues surrounding particular technologies or legislative provisions but that you would be pleased to arrange to provide expert advice on specific technologies. You can take this on notice, but it would be helpful if you could perhaps provide to the committee secretary a list of the sorts of technologies or experts that you could provide in that sense. Depending on who you have available, it might be useful for the committee at some future stage to have a look at some of these things, just to get a feel for some of the latest developments.

Mr Durie—I am not sure what is the best way of dealing with that. In Sydney yesterday morning we had a general briefing for our members on technology developments as they are panning out over the next 12 months. One of the key things that came out of that about

technology was that wireless is going to be huge, if it is not already, and that is going to lead to ubiquity of access, dispersal et cetera. If we think that a lot of people are online now and there are a lot of transmissions now, we have not seen anything yet. I am happy to provide a copy of that presentation to the committee. In terms of the advice we could provide, we would simply be drawing on our members who cover the whole field. I am not sure how we can articulate what that assistance is in detail.

CHAIR—What might be productive is if you, or one of your staff, get together privately with the committee secretary next week and talk through some of the things that you may have available, or your members may have available. We might pick the eyes out of that and perhaps say, 'These two or three might look particularly appropriate,' and then see how we might arrange for the committee to get a briefing. I think it helps us in conceptualising what our recommendations may be to actually have a bit of a practical understanding of what is out there. Looking can often be worth several thousand words.

Mr Durie—Yes, okay, I am happy to do that.

CHAIR—You might be interested to know, and I mentioned it to the previous witnesses, that for the first time this committee is having this hearing broadcast on the Internet, so you might be going around the world.

Mr Durie—Well, if it is over the Internet we are.

CHAIR—That is right. It just depends whether anyone is watching. Thank you very much for coming this morning.

[12.11 p.m.]

BLUCK, Mr Frederick Paul, Director, Policy, Commonwealth Ombudsman

MOSS, Mr Philip, Senior Assistant Ombudsman, Commonwealth Ombudsman

CHAIR—I now welcome the representatives of the Commonwealth Ombudsman. As I mentioned privately, Mr Moss has been to see us three times on different inquiries in a fairly short order, so welcome back. The committee prefers that all evidence be given in public but you may at any time request that your evidence, part of your evidence or answers to specific questions, be given in camera and the committee will consider any such request. As public servants you will not, of course, be required to answer questions that seek your opinion on the merits of government policy—if only! Mr Moss, would you like to make an opening statement?

Mr Moss—Thank you. The Commonwealth Ombudsman's interest in this inquiry relates to the first of your committee's terms of references; namely, whether the use of new technology by law enforcement agencies is adequately catered for by Commonwealth, state and territory legislation. Our interest is even more specific because the Ombudsman is concerned only about the actions of Commonwealth law enforcement agencies—at present the Australian Federal Police, and, following the recent bill, possibly the National Crime Authority—and the effect of their activities on members of the public. Our involvement currently occurs in three ways: firstly, dealing with complaints by members of the public about the AFP's law enforcement actions, and, as I indicated, that will extend to the NCA if the current bill passes; secondly, conducting, under the Complaints (Australian Federal Police) Act 1981, own initiative investigations concerning the Australian Federal Police; and, finally, inspecting the telecommunications interception records of the AFP and the NCA to ensure that those agencies have acted in accordance with the requirements placed upon them by the TI Act.

Law enforcement, necessarily, involves sensitive citizens' rights issues. It is an invasion of privacy for someone to enter a home or business, seize items to listen into a person's telephone conversations, monitor someone's computer, eavesdrop on someone's personal conversations or to take records of where they go and who they meet. In certain circumstances law enforcement bodies are permitted to intrude into the lives of citizens in these ways because it is accepted that damage done to society by criminal activity outweighs the infringement to personal liberties. But law enforcement agencies are subject to constraints imposed by the parliament and the courts. A court may reject evidence obtained unlawfully and officials can be called to account for the way they have used their powers. In the case of telecommunications interception, there is a legislative regime requiring that records be inspected to enable the public to be sure that actions taken were lawful.

Coming more specifically to our submission, our point is to suggest that it would be appropriate for a consistent approach to be adopted in the use of new technology by law enforcement agencies where a delicate balance needs to be achieved between the protection of citizens' rights and the wider public interest involved in providing to law enforcement agencies the appropriate tools to maintain law and order in the community. At present there is no consistent and equal requirement in relation to some of the technological tools used by law

enforcement agencies. For instance, provisions relating to the use of listening devices can vary between states and there is a special regime requiring AFP members to obtain warrants when using them for some purposes. The information obtained through a listening device may have a similar content or value to that obtained through telecommunications interception, yet the user of the device is not subject to similar oversight inspection. Another example is provided in the instance of emails where, for instance, to read an email not yet opened by a recipient requires a warrant under the Telecommunications (Interception) Act but to read an email that has been opened by the recipient requires a search warrant. In the former regime, of course, it is quite clear that inspections and a regime of accountability apply; in the second, as far as the Ombudsman's Office is concerned, none exists.

So there is real value, we submit, in a consistent accountability regime. Such regimes provide an assurance to the minister, and in turn to the community, that the agents are living within the law and respecting citizens' rights.

CHAIR—Could you tell the committee what sort of process or administrative-type problems or errors you have detected in your telephone intercept activity?

Mr Moss—I am pleased to say not serious ones, although we do provide a confidential report annually to the Attorney-General in which we outline in some detail what we do find. But our experience has been that any errors or problems identified during those inspections are quickly addressed and corrected by the law enforcement agencies. As a consequence, our inspections have been instrumental in bringing about changes to the processes that assist in maintaining compliance with the requirements of the TI Act.

CHAIR—Do you have any difficulties in your office in terms of technology expertise in this area?

Mr Moss—If you look at individual members, it is uneven across our office, but there is no doubt that we have a high level of IT expertise amongst some of our officers.

CHAIR—One of the points that has been made by other witnesses is they perceive that government generally is going to find it increasingly difficult to attract and keep people with appropriate technological expertise, not only for telephone intercepts but in other areas of new technology, partly because private industry pays better—and significantly so—but also because there are newer, more exciting and sexier things to do in a work satisfaction sense perhaps. Do you see that as being an ongoing problem for you?

Mr Moss—It certainly is an issue. It is an issue for me right now because over the last two or three inspections I had a two-person team which spends about two months per year on this inspection work. In one case an officer has been promoted and in another case an officer has taken extended leave. So I am faced with the prospect of getting a team together for the next inspection, which occurs towards the end of this financial year, and it will take some effort to do that to the standard that it has been done in the most previous inspections. So in the IT sense that level of expertise is very important and it is an issue.

CHAIR—Apart from just the expertise issue, which obviously we note, if, for example, your jurisdiction were to be extended to cover the use of surveillance devices to the NCA, would that present you with a broader resourcing problem?

Mr Moss—There would have to be consideration of additional resources, but in terms of expertise I think that would be beyond our capacity to organise.

CHAIR—Okay.

Mr SCHULTZ—Mr Moss, are you of the view that ASIO and the NCA are sufficiently comparable in role and function to justify an extension to NCA surveillance powers along the lines of those that ASIO possesses? Are they often not chasing the same targets as terrorists and organised crime groups merge their activities?

Mr Moss—I am aware of the NCA's interest in obtaining the powers that have recently been extended to ASIO, such as obtaining information on computers. I would be of the mind that law enforcement agencies should have the resources and the powers at their disposal to do the job required of them. What is necessary, though, is an accountability regime which provides assurance and public confidence that these powers are being used properly. In the case of the recent powers being extended to ASIO, I know—and you would know—that the inspector-general of intelligence and security has a monitoring role in relation to ASIO and the other intelligence and security agencies and, in fact, can provide that level of assurance in those particular powers and any other powers extended or given to ASIO. So my answer is, yes, those powers ought to be given, but I do think that the accompanying accountability regimes are necessary. As to the merits of the NCA and ASIO having similar functions and whether there is a case for that to be given to the NCA, I do know enough about that.

Mr SCHULTZ—Do you have knowledge of the extent of the successful implementation of the reforms in the 1999 ASIO Amendment Act in relation to its use of contemporary surveillance technology, such as the installation of tracking devices on people or in vehicles and remote access to computers?

Mr Moss—No, I do not know the extent of ASIO's use of those powers or much about them. I have just followed it from a general point of view. I formerly worked in the office of the inspector-general of intelligence and security and hence can speak from the oversight and monitoring point of view, but I was not in that office when those powers were extended to ASIO.

Mr SCHULTZ—In relation to audit responsibilities, if additional audit responsibilities were to be given to you, are the IGIS powers a suitable model?

Mr Moss—There has been quite a debate as to whether the NCA should have a monitoring oversight role, such as is provided by the inspector-general, or whether there would be a lesser role. I think it has come out of the debate that what was going to be sought in the first instance was a model where we, as the Ombudsman's Office, would be able to receive complaints about the activities of the National Crime Authority, but not have any further role—that is, not have any role in terms of monitoring and regular oversight. In that sense, it would be a reactive role that is being proposed for us at present. Of course, the exception to that rule is the specific

activity we do under the Telecommunications (Interception) Act, but that is inspection work rather than the more thoroughgoing monitoring that the inspector-general is able to do in relation to the intelligence and security agencies.

Mr SCHULTZ—Thank you.

Senator DENMAN—Mr Moss, could you tell me if in recent times there have been any cases, or examples of cases, where people have been surveyed using these new technologies, perhaps charged, and then found to be innocent?

Mr Moss—The short answer is no, but at this stage we have no power to receive a complaint from a person who believed that the National Crime Authority had acted improperly in this way, so that would be one issue. The second issue is that we have no responsibility in terms of monitoring that kind of activity.

Senator DENMAN—My concern was that, if that was happening, the records of those people, or inquiries, be destroyed.

Mr Moss—That may be one of the outcomes of an investigation we would do if we had the power to do it.

Senator DENMAN—We have heard recently from the NCA support for the UK's regulation of investigatory powers. Can you comment on how you see that as a model for Australia?

Mr Moss—We are not aware of that model, I am sorry.

CHAIR—It was an act that was passed last year, I understand, in the UK. We understand that in the United States the Congress has twice refused to extend the FBI's telephone tapping powers, particularly to digital networks as I understand it, because of their concerns about civil liberties and privacy concerns. Do you have any knowledge of those developments, or do you have any views on those developments?

Mr Moss—I have no direct knowledge of those developments. In my view, the extension of powers must be accompanied by an appropriate accountability regime and, if there was a mismatch there, then we would obviously express a concern. But I am not aware of the particular issues debated in the USA.

CHAIR—Coming back a bit closer to home, as I understand it the Wood Royal Commission made a number of recommendations in its report in 1997 on reform of the Telecommunications (Interception) Act, some of which have been acted on. The New South Wales DPP has suggested that the amendments have not gone far enough. Justice Wood, as I understand it, recommended that the Commonwealth should devolve appropriate legislative and administrative responsibility for telephone intercepts to the states. He also suggested that consideration be given to prohibiting the introduction of new technologies unless they had in-built interceptibility, with the carriers in fact bearing the associated costs—which would not have gone down well with our previous witnesses, I am sure. I wonder if you have any comments?

Mr Moss—I have an immediate response to the prospect of state agencies doing any oversight or monitoring work of Commonwealth agencies. For their part, any suggestion that the Commonwealth have that role in relation to a state agency is strongly resisted.

CHAIR—That is a real surprise.

Mr Moss—I think that if fair is going to be fair then it should be equal to all. We have clear standards in the Commonwealth but it is pretty complicated as it is. To have a patchwork system whereby state agencies could look at Commonwealth activity I think would be undesirable.

Mr SCHULTZ—Mr Moss, on page 4 of your submission, in the last paragraph, you make the comment:

> I would see a consistent approach to accountability as being appropriate in the use of new technology by law enforcement agencies, where a delicate balance needs to be struck between protection of the privacy rights of citizens and the wider public interest involved in providing to the law enforcement agencies the appropriate tools to maintain law and order within the community.

I have some concerns about privacy laws. Could you define, or give an example, of where privacy rights of citizens would be overridden by the wider public interest?

Mr Moss—I think that a clear case is the interception of telephone conversations for law enforcement purposes. The Telecommunications (Interception) Act 1979 starts with a very simple proposition, 'No-one will intercept the telecommunications of another person,' and from that point develops a series of exceptions which enable law enforcement agencies to do just that. So, listening in on someone else's telephone conversation is a clear example of a breach of privacy of a person, but giving law enforcement agencies the necessary tools to maintain law and order is the balance. The parliament has put in place very clear guidelines as to the circumstances under which telecommunications can be intercepted. Part of that regime is the inspections we do of the records which agencies are required to keep about those activities so that we can be sure, and the Attorney-General can be sure, that the agencies are using that power properly and in accordance with the law.

Mr SCHULTZ—Can I raise an example with you with regards to video surveillance? Video surveillance of drug operations may be undertaken through, say, a local government municipality on drug dealings within its local government area, which identifies a drug deal going down and shows a drug dealer selling whatever to a user. Under what circumstances should the user or the drug dealers' rights or privacy be respected? Do you think that under those circumstances, given the problems that we have with the distribution of drugs within this country today, either one of the two should be subject to any privacy rules?

Mr Moss—The privacy rule is encapsulated in the requirement by the law enforcement agency to obtain a warrant for that surveillance activity. I know there is some debate about whether video surveillance comes under the TI Act but it is the warrant obtained which gives the authority to the agency to do so and that gives the authority for the infringement of the privacy of those particular drug dealers.

Mr SCHULTZ—Thank you.

CHAIR—You mentioned earlier on what to my mind is the anomalous situation of how you would treat an email message one way if it had been opened by the recipient or a different way if it had not been opened by the recipient. What is the situation with mobile phones and the interception of conversations on mobile phones? There was a very famous interception that took place between a couple of leading political figures of the day, I seem to recall. I do not recall the media who published that all across the front-pages actually being prosecuted, but presumably it was a crime. Or was it not a crime? What would you do with mobile phones now that we have all these sophisticated messaging capabilities?

Mr Moss—This is a technology question for the law enforcement agencies to keep up with the changes in technology and the uses it is being put to for the purpose of criminal activity.

CHAIR—It is the first time I have ever known you, Mr Moss, to have to hesitate.

Mr Moss—I was just thinking of the need to distinguish between—

Mr Bluck—A mobile telephone service is as subject to a potential interception under a warrant as any other service and there are references in the submissions from other agencies to the use of person-based warrants which may track a number of services used by an individual. So I cannot see any reason why there would be much difference there.

Mr Moss—That is quite right. The only distinction between mobile telephone services and landline services, as I was saying, is the great ease now with which you can change the SIM cards in those phones. The problem is therefore for law enforcement agencies to keep up with it and devise responses to that improvement in technology. As to the famous conversation that you mentioned, I would say heaven help a law enforcement agency that disseminated the content of such an intercepted telephone call because very much part of the accountability regime is not only that you intercept in the first place, but there are very careful guidelines as to what you can do in terms of passing that information on to other agencies or within the agency itself.

CHAIR—I must commend Mr Bluck for the outstandingly straight cricket bat he provided to that question. The secretary whispered in my ear that Don Bradman could not have done better, but I think perhaps Geoffrey Boycott would be a better analogy. I have a mobile phone that is capable of taking messages. Can you detect whether a message has actually been opened and read or not read by me, and would that have the same difference in terms of how you dealt with it, comparing it to your earlier analogy about an email message?

Mr Bluck—Are you referring to, for example, SMS messages?

CHAIR—If somebody phones me and I do not answer they leave a message saying, 'Ring home urgently,' or whatever the thing is. I switch on my phone and there I have a message.

Mr Bluck—As I understand it, the interception is once the thing enters the telecommunications system. So it has gone into the system and at that point I suppose it could be intercepted under the TI Act, even before it has been heard by the recipient. But I do not know if this has ever come up as an issue.

Mr Moss—Not with us, no. As I understand the argument, it is not within the possession of the recipient until the recipient reads the message or opens the email.

CHAIR—Can I thank you very much once again for coming to talk to us. As usual, you have been very helpful and constructive and we are most grateful. Thank you. You will have seen that we tabled a report yesterday into the NCA Legislation Amendment Bill. Whilst there were some disagreements within the committee on some matters associated with the bill, we were unanimous that you were a very competent organisation to take over the independent review of complaints and so on.

Mr Moss—Thank you, indeed.

[12.38 p.m.]

EDWARDS, Mr Peter, Deputy Director, Australian Bureau of Criminal Intelligence

HEWETT, Mr Neville Allen, Manager, Information Services, Australian Bureau of Criminal Intelligence

HOLMES, Mr Mark Edward, Manager, National Intelligence Association, Australian Bureau of Criminal Intelligence

WARDLAW, Dr Grant Ronald, Director, Australian Bureau of Criminal Intelligence

CHAIR—I welcome the representatives from the Australian Bureau of Criminal Intelligence. I understand, Dr Wardlaw, that you have been in the job for about 2½ weeks, so you are obviously an expert on the subject! We look forward to an ongoing relationship with your organisation, not only for this inquiry but obviously for other matters in which we deal. The committee prefers that all evidence be given in public, but you may at any time request that your evidence, part of your evidence, or answers to specific questions be given in camera and the committee will consider any such request. We have received your submission and that has been published. Dr Wardlaw, do you want to make an opening statement?

Dr Wardlaw—Yes, thank you very much. Thank you for the opportunity to appear at this hearing. I welcome the chance to contribute to the review as I think the issues you are looking at are extremely important for the future of law enforcement in this country. Could I just start by very briefly giving a bit of background about the ABCI and our involvement in this issue. When the ABCI was established 20 years ago, we worked with eight police services; today we have in excess of 38 agencies with whom we exchange law enforcement information. I think this issue is important, not only because it identifies the growth of the ABCI and of law enforcement partnerships, but it provides an indication of the number of agencies in the Commonwealth and the states who now have some form of law enforcement role.

As you would already be aware, the role of the ABCI is to facilitate the timely exchange of criminal intelligence between law enforcement agencies and it does this at two levels: firstly, by maintaining and making available national information and intelligence systems which encourage law enforcement agencies to make use of and contribute information to a national criminal intelligence infrastructure; and, secondly, the ABCI undertakes a range of intelligence assessments and maintains a number of national projects. Our clients are able to use the information technology resources of the ABCI to restore and retrieve their information while aggregating their data with the collective intelligence holdings of other law enforcement agencies. In addition, our client agencies can access the services of a number of civilian and police criminal intelligence analysts, particularly in relation to ABCI national projects and activities.

While there have clearly been improvements in the willingness of law enforcement agencies to exchange a whole raft of law enforcement information, we believe there is still a very long way to go. Even today, with the lessons of the past not too distant, agencies still choose to

develop in-house intelligence systems in some cases, rather than embrace the collective approach that we certainly would promote. While I have no doubt that reasons can always be found to support these decisions, it strikes me that if law enforcement is going to remain effective in the future we need to agree on where expertise should best reside. Clearly, it is not in the long-term interests of law enforcement if every agency develops expertise in all fields of policing—I think you just have to look around at the difficulties that many police services are currently experiencing in trying to retain their trained investigators and computer crime experts in the face of job offers from the private, and in some cases public, sector.

I think we need to take a collective approach to these issues and seek solutions and a new range of agreements about agency specialisations, strategic alliances, and service agreements in the field of criminal intelligence systems. For example, we believe that the ABCI has the systems development and analytical expertise to ensure a product which is not only user-friendly and compatible with other operations but is easy for an analyst or an investigator to use and delivers a functionality which makes his or her job easier. The Commonwealth, the states and territories all have a substantial investment in our systems and its potential could, in our view, be more fully realised by further systems enhancements and resisting the proliferation of new systems.

Turning to the actual issue of technology and law enforcement, we see the issue of technology as posing significant challenges, but also opportunities, for the law enforcement environment in Australia. Of course, in many respects law enforcement is in a position no different from other sections of society: we have clients demanding increased and improved services with resources remaining static, and in some cases declining; we have law enforcement agencies competing for scarce public resources and agencies sometimes having to spread their resources too thin in order to retain coverage over a wide range of criminal issues; and there is pressure on law enforcement agencies to retain key and experienced personnel. I think we are all facing the sometimes unrealistic expectation that forensic science, through things like biotechnology, DNA and so forth, will solve everything, and, of course, things like globalisation, the information and communication revolution and the demands for individual and collective privacy that are often being exacerbated by those developments.

Law enforcement is often in the position of playing technology catch-up with criminals and criminal groups who are either using technology to give them an advantage in their illegal dealings or are making effective use of existing complexities in the technological and communications environment. We recognise that some of these issues are outside the scope of law enforcement on its own to address but there are obviously areas where we can and should be more effective than we are.

The ABCI has conducted a number of assessments which have revealed the role that technology is playing in the contemporary criminal activity. Some of the activities that we have examined in these assessments have been canvassed in our submission. These include things such as the uncovering of international child sexual abuse networks that saw potential members having to upload up to 10,000 images of child pornography onto the Internet in order to gain membership; the use of chat rooms and web sites that describe the manufacture and availability of drugs; a range of frauds and other financial offences covering areas such as bogus invoicing, plastic card fraud, with large losses, in the billions sometimes, being mentioned by major corporations; and, increasingly, identity fraud is a major issue. We also have web sites being

used by criminals to attract membership to outlaw motorcycle gangs, software and music piracy estimated to be costing the industry US$11 billion per year, miniaturisation of weapons, and mobile phones and emails to commit crimes.

On the other hand, technology is a critical part of modern law enforcement. We obviously have everyday things like word processing and spreadsheets for use in analysis and prosecution, software programs being developed that map criminal activity and that give spatial and temporal behaviour patterns as well as indicating offender behaviour, improvements in surveillance technology, including listening devices and telephone interception, mobile phones and emails helping officers to continually keep in touch, and, of course, national systems such as CrimTrac and our own intelligence and information systems.

Since preparing our submission, a number of law enforcement agencies have identified further concerns, in particular in relation to telecommunications, and, while these areas are to some degree not new, they are presenting increasing difficulties, particularly to state and territory policing. They include areas such as number transportability, the use of SIM cards, the cost to law enforcement of accessing information from the integrated public number database, call charge records, the variable costs of accessing service provider records from the proliferation of service providers, and time delays in serious and sensitive investigations. I think we just wanted to flag here the fact that while the details are still being worked out, the ABCI is considering a request from both state and Commonwealth agencies that we undertake a review of the full impact of these and possibly other telecommunications issues from an intelligence point of view.

I thank you for the opportunity to appear here today and I and my colleagues would be happy to answer any questions that you might have.

CHAIR—What is the relationship like between ABCI and the NCA?

Dr Wardlaw—I think we have had a very productive relationship with the NCA. Our dealings are primarily with the intelligence area and some of the national task forces. The ABCI provides, through its Australian criminal intelligence database, the repository for a lot of the intelligence holdings that come from the task forces. We certainly have been involved with the NCA over the years in a number of joint assessments on some important matters. Just yesterday I had the first of what I think will be a series of discussions with the director of intelligence about making sure that the relationship from here on continues to develop and that we clearly identify those areas in which we can add value to each other's processes.

CHAIR—Could you comment on how CrimTrac and ALEIN relate to teach other? Do you see potential difficulties of turf battles?

Dr Wardlaw—Again, I have already had discussions with Jonathon Mobbs, the CEO of CrimTrac, to try and ensure that in fact we do not get into any sort of turf battles with that organisation. I think we serve different, but complementary, purposes, and I think we have already agreed on some basic elements to the working relationship. I would ask Mr Hewett to expand on that as our expert in the area.

Mr Hewett—Recently I have had some discussions with the consultants from CrimTrac and the view is to look at how they can better serve the supply of intelligence to the ABCI through the CrimTrac medium. At the same time, we are going to look at some business issues of how we can actually enhance CrimTrac's delivery, through our product being passed back to CrimTrac. There are a whole range of security and need-to-know issues to be worked through, but certainly we can add value to the CrimTrac process and we believe that we can be complementary through interoperability.

Mr KERR—In terms of this strategic overview role that you are playing—and I think you indicated you may be seeking to do that review of the impact of technologies across jurisdictions—we had earlier evidence that there needs to be greater cooperation in dealing with cybercrime across all jurisdictions, and making the obvious point that these are borderless crimes, both within Australia and external to it. Do you have a growing awareness of the need to develop a coordinated approach nationally and do you also have any outreach to similar bodies in other countries, because the border issue is not just an internal issue; it is an issue which presumably now means that we need to develop strategic linkages and interoperability with law enforcement and intelligence organisations in other countries.

Dr Wardlaw—Yes, certainly. In the last couple of weeks since I have taken over we have already had internal discussions building on work that we had already launched in the fraud area in recent times and expanding that to encompass a much wider range of e-crime issues generally. At this stage we are examining exactly what the priorities are for the collection of intelligence in that area. As I think you have correctly identified, we are not seeking to become the overall experts on everything to do with e-crime, but to start slowly and build on those areas of expertise, particularly in the fraud and financial crime areas, that we already have, but also enter into alliances with other organisations, such as the Australasian Centre for Policing Research which already has a role in that area, and certainly draw on the growing interest in the state and territory police forces where we are starting negotiations with a number of similar national criminal intelligence bodies overseas. I have already had some discussions with the Canadian service and hope soon to have some with the National Criminal Intelligence Service in the UK, which has already developed a considerable start in the cybercrime area. So we recognise that as a priority issue and we are assigning internal resources to it. But obviously if it is going to develop into a much wider and broader role we are going to have to look at additional resources, both in collection and, more importantly, in analysis.

Mr KERR—Can I ask you what happened to the Office of Strategic Crime Assessment and the role it was proposed to play in relation to long-term strategic policy setting? Is that a role that you now play and what happened to the structure that was in place previously?

Dr Wardlaw—The Office of Strategic Crime Assessment still exists, and, in fact, is about to engage in a renewal of some of its assessment activity, but I would again see us as being complementary. The OSCA role is very much looking at about a five-year time horizon, primarily in Commonwealth law enforcement interests, but obviously the assessments that they put out also cover the same sorts of areas of interest that impact eventually on state and territory policing particularly. We see ourselves as occupying a strategic role for policing, and particularly state and territory policing, probably looking at one or two years out. I think that is the focus that is most appropriate and would be most welcome by the police commissioners. Again, I have already had some preliminary discussions with the director of OSCA about

making sure that we feed into each other's processes and that although we have similar interests we are not covering the same ground.

Mr KERR—You will have to treat me as ignorant because, I am sorry; I have obviously lost a wee bit of immediate familiarity. I have not seen anything of the product of OSCA for many years—they published some materials early but I certainly have not seen any, either provided in the public domain or in confidence to this committee or any other committees on which I have served. I thought it had withered on the vine, a bit like CLEB. Can you tell us what is the state of play with those two agencies, CLEB and OSCA? What is their staffing and what are they doing?

Dr Wardlaw—I have been out of the law enforcement area for the last year, since I left OSCA, so I am not exactly sure of what CLEB itself is doing now. OSCA certainly has been recruiting in the last couple of months and I think is back up to strength again and has an analytical program ready to start off. I understand there are a number of assessments that are due out soon from work that was done last year and certainly prior to that assessments were coming out still on a regular basis.

Mr KERR—So the baby still breathes.

Dr Wardlaw—It still breathes.

CHAIR—I think Mr Kerr is probably suffering to some extent from that disease described by one of his former colleagues about relevance deprivation syndrome since he left government.

Mr SCHULTZ—I notice on page 9 of your submission there are a considerable number of points relating to paedophilia and child sexual abuse in Australia. Part of one of the latter three points reads:

> ...While each jurisdiction has legislation for possession and distribution of child pornography, it is considered to be ineffectual.

The next two points read:

> it is rare for offenders convicted for possession of child pornography to be sentenced to imprisonment in Australia. While this is also generally the case overseas, in the UK for instance it is not uncommon for most offenders to be placed on the sex offender register; and
>
> it is generally agreed within law enforcement that a dedicated agency is required to target internet child pornography. This would provide more efficient use of resources and foster coordination of investigative and intelligence expertise.

I have two questions. Firstly, given child pornography and child sexual abuse are seen by the public as abhorrent, what do you feel is the most compelling factor behind what is publicly perceived as soft sentences towards predators of children and which you have covered in one of those points that I just mentioned? That is the first question. The second question is: what role—and I do not have any problems with this—would a dedicated law enforcement agency play in terms of getting on top of the Internet child pornography industry, apart from more efficient use of resources, and how could it influence the role of the judiciary in making it far more appropriate for them to administer penalties on those people in line with public expectations?

Dr Wardlaw—I might ask my colleagues who have supervised the actual production of that report and are familiar with the details to comment on that.

Mr Holmes—Can I answer your second question first. In relation to a new unit, we were talking about greater coordination, again, between law enforcement. We have several state jurisdictions within Australia which are currently working on child Internet pornography and have officers working undercover attempting to identify paedophiles and their activities. These officers are engaged out in the broader Internet in the chat rooms. We have no evidence to suggest that it has happened yet in Australia, but we do know from the States that it is possible to have two law enforcement officers talking to each other, each believing the other person is a paedophile.

CHAIR—That is called an embarrassment, is it?

Mr Holmes—It is unfortunate, and for reasons of operational security jurisdictions are quite loath to make generally available the details of such operations. A national register kept at an appropriate security level by appropriately cleared people could be one means of overcoming this. There is also the problem of different legislation in different jurisdictions in Australia making it an offence for law enforcement officers to actually upload pornographic images. Law enforcement officers in the drugs area are allowed to engage in properly controlled deliveries of narcotics in order to apprehend offenders. In most jurisdictions in Australia it is not possible to do that with child pornography, even if the images are not actually of children but altered images of consenting adults. The paedophile networks throughout Australia and overseas are quite well aware of the restrictions that are placed on law enforcement officers and therefore one of the first demands that is often made when someone approaches these chat rooms is, 'I want to see your images, put them up.' If law enforcement cannot do that, then that is the end of that investigation in many instances. In relation to the sentences that are received, that is beyond the scope of the ABCI and reflects the parliaments of the various jurisdictions in Australia and the legislation that they pass for the judiciary to implement.

Mr SCHULTZ—In relation to your call for funding, you have raised the issue of accountability provisions, such as freedom of information, privacy, telephone intercept information, and the requirements to restrict data collected by the use of coercive powers. You also say that the accountability provisions place a burden on agencies that are increasingly unwilling to share information via the ABCI databases. Is there a practical solution to the problem and do you agree that the Commonwealth Ombudsman's role should be expanded to cover the oversight of all surveillance-type activity by law enforcement?

Mr Edwards—In relation to the first question, I suppose you have the difficulty about state autonomy in relation to the laws throughout the country and whether they would want to entertain that sort of oversight of surveillance activity. Could I ask you to repeat the first part of the question again?

Mr SCHULTZ—Just the lead-up?

Mr Edwards—Yes.

Mr SCHULTZ—The issue of accountability provisions, such as freedom of information, privacy and telephone intercept information.

Mr Edwards—The point I wanted to make there is that when we were created 20 years ago it was mainly to facilitate the sharing of police information. Back then many of the law enforcement agencies and other laws that exist today did not exist—the NCA did not exist when we started 20 years ago; apart from the crime commissions in New South Wales and Queensland, the Criminal Justice Commission did not exist; AUSTRAC did not exist; a range of ombudsman's offices did not exist; likewise the ICAC, the Western Australia Anti-Corruption Commission. So back then it was probably very easy for the police to say, in principle, 'Yes, we'll share information,' because there were a lot less constraints. But, when you think about the legislation that has been created since then, there are a range of constraints on those other agencies that have a law enforcement responsibility and in working through that it is always a difficulty to just throw things into the big bucket, which I suppose is what we are in very simplistic terms. I think there is always a solution and I think there are always ways of working around it, but one of the things that we do need is that resolve—and probably that resolve from governments—for all those organisations to willingly explore the options to share better.

Mr SCHULTZ—You do not need to respond to this, but what you are saying, basically, is we should perhaps concentrate our energies on political incorrectness rather than the political correctness which is creating impediments for our law enforcement agencies.

CHAIR—You did indicate that he did not have to respond and that is fine.

Mr Edwards—Can I say, a very interesting statement.

Senator GREIG—I am not sure these are the kinds of questions best directed to you guys, but I have an interest in electronic crime and the Internet in general. Do you have evidence that there is an increase in electronic crime within Australia and, if so, to what extent?

Mr Edwards—I do not think there is much doubt about that. I guess our particular area of expertise at the moment relates to fraud, and there are a whole range of new modus operandi appearing all the time. We have probably all heard of the Nigerian fraudsters who are now targeting people via the Internet. We are aware of significant crime committed by international groups in Australia skimming the identifications from credit cards, and I suppose simply the fact that this committee exists and the fact that the police commissioners in Australia have identified it as such a significant priority are all supporting data and evidence that it is a growth crime activity.

Just to put things in perspective, when you talk about e-crime, in a lot of ways it is just using a new mechanism to commit traditional crimes. At the end of the day there are probably two major crimes in our society, theft and assault, and most crimes will fit into a whole range of different variations of those. What we are confronted with is a whole new range of ways for people to steal or to put people in fear. So, in answer to your question, yes, it is a growth area.

Senator GREIG—Is it a question also though of greater accessibility? I am a relative newcomer to Net banking, for example, but I now use it quite a lot—it struck me the other day

that I have not actually set foot inside a bank for some months, simply because the accessibility on the Net is so easy. But at the same time I feel a sense of discomfort and vulnerability when I am sitting there paying bills and whatever, because all my information is on the screen and you get a sense that someone else may be able to access that, as they do with credit card details. Do you have a view that the protections that the banks say they provide to privacy are adequate? Do you have examples where that has been breached?

Mr Edwards—Let me just say, if you have not been in a bank for some months, do not go there at lunchtime on a Thursday. There are examples in relation to the question, but I think we would probably prefer to take that on notice so that we could provide a more accurate response to the question.

Dr Wardlaw—Can I just add to that. I think there are two other considerations that are implicit in answering your question. The first is that there is the accessibility issue, so a lot more people are able to commit old crimes using this new technology because the systems are available to more people. But I think also because of the pervasiveness, particularly of electronic systems, the amount of damage that can be done by an individual or an organised group is much greater than it possibly was in the past. The financial losses can be much greater, particularly when you are talking about the threat to the national information infrastructure, but the social and other damage that can be done is also theoretically very large. So it is the potential damage and the reach of any individual criminal that are factors that make this something that we have to take more seriously.

Senator GREIG—Can I ask about hate crimes and hate speech and the use of that on the Net. I was visited recently by some lobbyists from Canada—and I think Mr Edwards mentioned Canada earlier—who appear to be at the early stages of trying to develop some kind of international recognition of this dilemma. They used an example where a particular hate site had been created in the US but was going through an ISP in some other country, being downloaded in yet another country and from there passed on, and the areas of jurisdiction become very grey. They were concerned that the incitement to violence was now so much easier to do over the Net and that Australia, amongst other countries, needed legislative responses to that. Is that something to which you guys have turned your mind or that you are at least aware of? Are you nodding an indication?

Mr Edwards—What I am nodding at is an indication that I am aware of the issues that you have related from the US and Canada, but it is not something that the ABCI has specifically investigated. However, as you were talking it exercised my mind to the fact that, although we are aware that hate organisations have existed in countries like the US for some years, from what you say, if they are now moving that on to the Internet it makes it far more accessible, just like other sorts of gangs we saw existed in the USA many years ago and we now have in Australia and have had here for a long period of time. So I guess we can never ignore those developments internationally in Australia but it is certainly not something that the ABCI has specifically inquired into in recent times.

Senator GREIG—You talk also in your submission about the availability and increase in piracy in terms of CDs and software. Are your referring there to piracy in the sense of the actual physical product or Internet transmission? I am thinking in the context of the Napster debate—I understand from a recent court ruling in the US that Napster is to be closed but my instinct is

that someone will step into its place. The issue of Internet product and access to Internet product is going to be one with which governments may not be able to grapple. Do you feel that the piracy industry—if that is the term—that exists will evolve into an electronic industry and there may be legislative approaches needed to address that?

Mr Holmes—We have done some basic research into those areas you have just talked about and a large proportion of it falls within copyright, in which civil actions are available to the owners. The primary concern that we have at the moment is that criminals can view these areas as being exceptionally profitable and be able to move in and deal in these sorts of areas. Again, it is a matter of resources and hierarchies in determining priorities within the bureau and reflected by our clients and it is an area which is growing in importance in the state and territory jurisdictions.

Senator GREIG—Thank you.

CHAIR—There is a commercial software company called The Distillery which has submitted to us that your in-house database, ACID, is a limited product that is inferior to The Distillery's own commercial off-the-shelf product called InterQuest. It is also critical that you have an unfair commercial advantage over them in that you are offering your product free to other government departments. Would you like to comment?

Dr Wardlaw—I will defer to Mr Hewett who is responsible for that, but, in general terms, obviously all organisations that are offering products think that their product is meeting the market need. We certainly have a lot of very satisfied customers but I do not think we are in the business of being competitive with industry. We are in the business of trying to provide a national, integrated system, and it is being paid for both by the Commonwealth government and the states and territories and so directly funded in that way. But I might ask Mr Hewett to address the specific issues.

CHAIR—It is called a death pass, I think.

Mr Hewett—I think the intelligence database is a very limited market and The Distillery is obviously targeting that. A lot of their expertise has come from ex-ACBI employees. We are not reselling out in the commercial market. Our focus in providing ACID principally, and ALEIN, as systems to law enforcement is to further the ABCI's objective in terms of facilitating the integration and sharing of intelligence. From that perspective, yes, I suppose they can say we are competing and maybe denying them business opportunities, but we also are looking at it from the point of view that the ACBI is actually going through a resource issue. Just recently we have been introducing user-pays, and at a moderate rate, in order to further the developments and the improvements to the systems and further the capability of law enforcement.

Mr KERR—I think it was Mr Edwards who mentioned that there was some complexity about information exchange across jurisdictions because of the different constraints of what material could be released and made available to you. I found that very interesting because it is probably not something that I have given a great deal of attention to. I was wondering if the ACBI has looked at whether or not there should be some recommendation to governments about this issue, because we all have common concerns about privacy. We have gone through an

attempt to get a national scheme up on forensics. I do not think anyone wants to prevent the free exchange of information about criminal intelligence and material that would relate to better law enforcement, and yet everybody does want to put proper restrictions around privacy and improper release of this material. But if the rules are meshing as an unintended consequence it may be something that needs our attention. Is there attention being given to what legislative response might be appropriate to try to make sure these systems can be integrated and streamlined, because it seems quite silly to approach policing now at a national level otherwise than as a cooperative effort?

Secondly, has any advice been taken as to whether or not it would be within the Commonwealth's legislative competence to establish a common framework that would be constitutionally valid to provide an overarching framework whereby such exchange could occur?

Mr Edwards—I suppose the short answer to your question is no, in that we have not actually explored that at the moment. I suppose, to be fair, the reason would be that we would rather try and work those through with the respective clients, certainly in the first instance. To be fair, some of those organisations have very definite legislation that, for a number of good reasons, will prevent them from sharing information. Probably one of the reasons why we would go about it this way is that we are an organisation set up by consensus and not set up under legislation ourselves, although we do get a mention in different bits of legislation now. I think it is something that ought to remain on the agenda, and probably just in these discussions now there is potential for exploring and better articulating the issue. But I think in the answer I gave before there could be opportunities to improve that through enhanced cooperation and a will to explore that by the agencies themselves.

Mr KERR—I do not want to suggest in any way that there should be an imposed solution, but I suspect that no-one amongst the states or territories or Commonwealth says, 'We have an interest in impeding the effective communication of information,' so, to the extent they do, they do so either inadvertently or because they are claiming that there is a general principle involved which ought to apply to particular classes of information. But presumably this ends up being a bit labyrinthian, and I think that was the suggestion you were making. If you are not doing work in this area, does anyone do work in this area? Going back to the chair's comment about relevance deprivation syndrome and the eternal quest of parliamentary committees to do something that is useful, productive and constructive, is it a task that a committee such as ours might usefully look at in terms of commonality of information exchange?

Dr Wardlaw—I think it is probably timely because one of the things that has happened is the accretion of many of these regulations over time without thinking about the implications for other areas. So there are very good reasons in that specific area, but not necessarily having thought of the second order of things. What we need is some sort of an overview of what we are trying to achieve by all of these things and whether there are exceptions that can be made for specific purposes. Because it crosses a fair range of responsibilities—telecommunications, law enforcement, privacy and so forth—I think there is probably no individual bureaucratic body that is responsible for dealing with those sorts of things, so that would lead me to the view that probably a parliamentary mechanism is the appropriate one.

Mr KERR—I assure you that this committee and its members are in no great rush to commit themselves in detail to intensive work in committees over the next nine months. Other events may be given priority—

CHAIR—And after that, when you are still suffering relevance deprivation syndrome—

Mr KERR—After that, when the chair is the deputy chair, he may wish to renew the venture. But it may also be something that, with your interjurisdictional hat, you may be able to stimulate or kick off some discussion about, because, frankly, until Mr Edwards raised that I had thought that in most of these areas there were law enforcement exceptions—and in fact I know that in many there are—and I had not really thought that this was a difficulty.

Dr Wardlaw—I think there are certainly things that the ABCI could do in our area of interest, but it is a lot wider than that as an issue for law enforcement as a whole.

CHAIR—Going down perhaps another strand of this problem of fragmentation and growth of agencies, which I think you referred to in your earlier comments and which has come up time and time again with different witnesses, allied to the problems of expertise and shortage of supply of skilled expertise in what you might call the cyber forensic area, the NCA has actually put in a funding bid to set up a cyberforensic unit. We read in the media—and, of course, we all believe what we read in the media—that in the US, for example, they have committed a huge amount, $80-odd million, to set up some new super-duper centralised body; I think it is called Desert Storm. In the UK they are setting up a central body to tackle web-based fraud and things of that sort, and again, something like £25 million has been put into that. Would you have a view as to whether Australia would benefit from a specialised cyberforensic capacity and, if so, where would you see it being located? Do you have any feel for how much it might cost? You can take that question on notice if you wish.

Dr Wardlaw—We certainly do not have any estimates of how much it might cost, and I think we would certainly like to take the detailed answer on notice as well. But, in principle, yes, I think we need it. It is an issue of such growing importance and potential damage to the economy that we do need to have the capacity. There are a number of models of developing that capacity, whether it be an agency that is dedicated to it or more lateral thinking about some virtual capacity that utilises the specialist expertise of a number of organisations. I think the only thing that we would probably like to say here is that we have, in ACID and ALEIN, the basis for a lot of the information and intelligence requirements of that system. We probably have the core of the intelligence component for such a capacity and we would like to see the ABCI's services used in any new initiatives, but it does not have to be a particular organisation or one organisation that tries to do everything.

CHAIR—I think your comment about a virtual organisation is interesting. If you could develop that further on notice, by all means, but that would be an interesting concept, which I would certainly like to have a good look at.

Dr Wardlaw—Yes, certainly.

CHAIR—If there are no further questions, could I thank you very much for coming this morning. It has been very helpful. I am aware that we have a raincheck with you to come and visit your organisation—I do not know whether you are aware of that.

Dr Wardlaw—I certainly renew the invitation.

CHAIR—That concludes today's hearing and I would like to thank our witnesses, *Hansard*, the members of the committee and staff for coming.

Committee adjourned at 1.36 p.m.