COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE ON THE NATIONAL CRIME AUTHORITY

Reference: Law enforcement implications of new technology

MONDAY, 2 APRIL 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

Monday, 2 April 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 George Campbell and Denman and 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 9.36 a.m.

KEELTY, Mr Michael Joseph, Acting Commissioner, Australian Federal Police

FAGAN, Ms Audrey Ann, Acting Deputy Commissioner, Australian Federal Police

WILLIAMSON, Mr Gordon James, Director, Technical Operations, Australian Federal Police

CHAIR—I declare open this fifth public hearing of the parliamentary Joint Committee on the National Crime Authority inquiring into the law enforcement implications of new technology. I welcome our first witnesses today, who are from the Australian Federal Police. We have received the AFP submission, which was forwarded by Mr Keelty last August and has already been published by the committee. I also note that we received from Mick Palmer—the former AFP Commissioner and chair of the police commissioners conference which established the Electronic Crime Steering Committee—a copy of the report from the Australasian Centre for Policing Research. The report is entitled *The virtual horizon: meeting the law enforcement challenges* and focuses on developing an Australasian law enforcement strategy for dealing with electronic crime.

I should also record that Mr Keelty joined members of the committee late last year on an inspection tour of the AFP's Forensic Services centre in Weston. During that tour we were shown many of the new technologies which the AFP has available to it to assist in its fight against crime. I will publicly record my personal thanks to Dr James Robertson, the centre's director, and his staff for making it such an informative and enjoyable visit.

Mr Keelty, as you are aware from previous appearances before the committee, we prefer 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 give consideration to any such request. Before I invite you to make an opening statement, I understand that you have for the committee some material requested at a hearing last December when Mr Mark Walters appeared briefly before the committee on the AFP's behalf. I invite you to make an opening statement.

Mr Keelty—Thank you, Mr Chair. The AFP welcomes the opportunity to contribute to your inquiry into the law enforcement implications of new technology. As the committee is aware, the AFP submitted its own submission in response to the inquiry terms of reference and contributed to the Attorney-General's Department portfolio agency submission as well.

The AFP, as the Commonwealth's primary law enforcement agency, is acutely aware of the challenges the current technology environment poses to law enforcement and the interests of the Commonwealth. The rapid and ever-increasing advancement in new technologies is one of the principal drivers of globalisation. Within the law enforcement environment it also drives the growth in transnational crime, the facilitation of traditional crimes by a more sophisticated means and the emergence of new crimes, such as those associated with the Internet. It goes without saying, therefore, that those advancements provide enormous challenges to law enforcement. Before providing the committee with some remarks on the implications of new technology on law enforcement, I would like to make some comments in relation to the

cooperative arrangements enjoyed by Australian law enforcement. Similar arrangements also exist between the Australian Federal Police and our international law enforcement partner agencies, which now extend to many corners of the globe.

On 15 March this year, I appeared before the Senate Legal and Constitutional References Committee. The committee is inquiring into the management arrangements and the adequacy of funding in the Australian Federal Police and the National Crime Authority. In appearing before that committee, I spoke about the strong relationship that exists between the AFP and the NCA. Our strategic partnership and high level cooperation has resulted in excellent operational results. There is now universal recognition that law enforcement cannot meet the challenges of the current criminal environment in isolation but must maintain cooperative and collaborative alliances to ensure that we provide the level of response and service we are mandated to provide.

As the longest serving member of the AFP ever to be seconded to the NCA, I would make the following statement. The AFP enjoys a close strategic partnership with the NCA. The majority of the NCA's investigators are AFP federal agents. Several former senior AFP managers have been employed by the NCA in key positions. The AFP believes it is appropriate for the NCA to exist as an independent agency. It is inappropriate for any police organisation to have the special powers conferred upon the NCA. In short, I believe the cooperation that now exists between the NCA and the AFP has reached an all time high. I include in that my own relationship with the chairperson and members of the authority. The AFP has also entered into memorandums of understanding and/or service level agreements with most, if not all, of its key partner agencies and stakeholders to improve the level of cooperation and service between the respective agencies. This has resulted in closer cooperation on a range of issues, including information intelligence sharing and exchange as well as the provision of specialist services to stakeholder and client agencies.

I take this opportunity to raise the matter of recent media speculation concerning the merging of the AFP and the NCA, which may have come to the notice of the committee. Such speculation was highlighted in a recent article which appeared in the *Canberra Times*, referring to public hearings of the Senate Legal and Constitutional References Committee mentioned earlier. In response to that article, I wrote a letter to the editor in which I expressed in clear terms that the relationship between the AFP and the NCA had never been better and that we enjoyed a number of recent successes in targeting organised crime groups. I would like to reiterate those comments to the committee today. The AFP has never had an intention to do anything further than, where appropriate, complement and supplement the work of the authority. I repeat that it would not be appropriate to vest those powers into a police agency, and commentators would do well to recall that state and territory police agencies are also essential elements of the National Crime Authority.

I would now like to comment on the technical issues that the committee has been examining during its inquiry. It is firmly the AFP's view that the future is in technical advancement. Having attended a number of international meetings on the use of technology to combat crime, I can tell you that the AFP and the NCA are far further advanced on this aspect than many other law enforcement agencies around the world.

CHAIR—I am not so sure that is a comforting statement. Sorry, I should not have interrupted.

Mr Keelty—In joining the issues of technology and the AFP/NCA relationship, I can advise the committee that the AFP and the NCA work closely together and are currently examining proposals for the integration of some specialist technical teams to ensure closer cooperation and the streamlining of operational resources. One example of relevance to this committee is the work progressed through the AFP/NCA board known as TIES, which is the Telephone Intercept and Electronic Surveillance Committee. Until recently I have been an active member of that board. The intent of the board is to deliver within the next 18 months a joint facility on telephone intercept capability. That facility will have the capability to be extended to electronic surveillance—the intention of which is to deliver live data to the work place of each and every federal agent or investigator in the NCA. Another important aspect for the AFP has been the upgrade of the forensic facility at Weston, which you mentioned earlier, Mr Chair. Traditionally we were also funded to establish some new electronic evidence teams around Australia. They represent at the moment our capacity to deal with electronic crime.

There is currently a whole of government approach being taken to the issue of protection of the national information infrastructure which relates to electronic crime. We are participating in the development of that. The AFP is involved in a number of diverse fora involving new technologies and, in many instances, is a key player in the development of strategies. The committee is aware, as you mentioned, Mr Chair, that the recently retired Commissioner of the AFP, Mr Mick Palmer, was the chair of the steering committee of the police commissioners conference electronic crime project.

I can inform the committee that as a result of the meeting of the Australian Federal Police commissioners in Papua New Guinea last week, the AFP Commissioner will maintain a position on the Electronic Crime Steering Committee, which is held under the auspices of the police commissioners conference. The steering committee has produced a comprehensive report called *The virtual horizon: meeting the law enforcement challenges*, which you mentioned earlier and of which you have a copy. This report has been widely circulated within the law enforcement community as well as both the public and private sectors. It is now a key reference for law enforcement agencies in their response to the e-crime environment. Three weeks ago the commissioners released an e-crime strategy. The AFP retains a key role in the working party and the development of action plans which are contained within the strategy. I would like to provide the committee with a hard copy of the electronic crime strategy, again produced under the auspices of the police commissioners conference by the Australasian Centre for Policing Research. It is available on our web site. That concludes my opening statement.

CHAIR—It seems to me that one of the recurring themes that has come through from a number of witnesses is the difficulty with the different stage of the development of laws in the states. I wonder if you could comment on the difficulty of the lack of harmonisation of legislation in the states, particularly in relation to the area we are talking about.

Mr Keelty—It is an issue of concern. It is one that I discussed at some length with police commissioners in Australasia and the South Pacific last week. The MCCOC report has been produced. I am sure the committee is aware of that report. What the states would like is for the Commonwealth to take a lead role so that the legislation is harmonised in terms of what the states now move to introduce. So it is an issue of concern. We are now trying, or I am as a Commonwealth representative, to approach the department to get some coordination and use the Commonwealth legislation as the head power, because there are jurisdictional difficulties that

are associated with technical communications. So other than to say that we maintain a key role on that steering committee and also a key role in the working group—which has now been formed to develop the strategies, one of which is legislation arising out of the e-crime strategy—I think we are of a like mind as the committee. We need to have some harmonisation and make sure everyone is moving as one, otherwise we will render one jurisdiction more vulnerable than another.

CHAIR—One of the other recurring themes that has come out has been the problem of expertise within the various agencies and bodies. Not only does there appear to be a significant shortage of expertise but, once you start to develop it, the people go off and get better pay somewhere else. Could you comment on how that has affected you and what would you see as potential solutions? Do you see it would be necessary to bring in consultants for a limited period of time or do you see the setting up of some central body that might provide expertise to all the organisational forces as being relevant? I am just interested in how it has affected you and what you see as potential solutions.

Mr Keelty—I will let Mr Williamson go into some of the detail of that, but what I will say in response to that is that we are now sitting in 2001. I suspect in the last five years we have seen peaks and troughs in terms of the expertise coming into and out of our organisation as we have home-grown the expertise. By and large the impact has not been as great as what we might have first thought. My belief, though, is that if we were sitting here in 2020, what we would see is a greater level of the same expertise within the community, so that the demand for the expertise would not be peaking as it is at the moment. Right at the moment, the expertise belongs to a small group within the community. As that becomes broader, the impact on organisations for mobility of people around the groups that have the expertise will have less of an impact.

CHAIR—So you need a short-term strategy until you get to that stage.

Mr Keelty—That is right. I think we have to take a long-term look at where this is all heading and how we are going to get there. Mr Williamson might have more details on the actual staffing arrangements.

Mr Williamson—I think the first point is to ask an objective question: are we achieving our goals or not? The reality is that, despite some speculation in the media, we have not been in a situation where we have not been able to successfully resolve an investigation because we lack the investigative expertise. All the way along we have either had internally, or through relationships with our partner agencies or other private industry sectors, the right level of expertise to bring to bear on the job at the time. We are quite confident that we will be able to continue to meet those demands into the future.

As part of that we have a process of upskilling all of our investigators, all of our federal agents, so as to enable them to better handle a digital crime scene. When many of us were trained, the crime scene was a physical place; it had lots of tangible characteristics about it. More often than not, you had a victim as well. Today the crime scene is increasingly electronic, be it in a traditional crime or in some of the new crimes. We recognise that we need to upskill our investigators so they can handle that level of activity. That process is well developed and there has been some considerable work between the AFP and all state police agencies to develop common competencies so that all police in Australia will have that basic capacity.

We recognise that above that level there are two other levels of expertise which are required. They are encapsulated in the e-crime strategy documents. One is the forensic examiner type role. Just as most of our investigators today know what a fingerprint is and know how to preserve a scene to preserve fingerprints, they do not actually have the skill to take them or analyse them. Another is in the computer environment, it is the same situation. The investigator will be expected to secure a scene and deal with it appropriately and, in some instances, get some expert assistance. Whether that is provided within each agency or a shared resource is subject to review under the strategy. There is also very high level technical expertise, which no agency could justify having on tap all of the time. We would approach that on a case by case basis. So if we are to look at a high level attack on a banking system, we would actually need to contract in the expertise of those who are at the cutting edge in that area.

So my belief is that we are getting there. Certainly it is a cooperative arrangement. The whole thrust of the papers coming out of the police commissioners conference talk about a cooperative relationship between law enforcement, which owns one part of the problem, and the industry itself, which provides the services, and the industries which actually use the services. Everyone needs to be working together. The last point the committee ought be cognisant of is whether the people who are making assertions about our levels of capacity actually have some other motivation in making those assertions.

CHAIR—What about the overseas experience? You mentioned earlier that we are in better shape than many and I rudely interrupted you. That would imply that they are not doing too well overseas. I would have thought in places like the States, for example, they would have been fairly well advanced in terms of technology and so on. Is that not the case?

Mr Keelty—It is certainly not in my experience. I have studied in the States with the FBI, and I have been amazed at the lack of advancement that there has been on the technical side in terms of Internet crime. That has improved since they set up their equivalent of a national cyber crime centre, as they have in the UK. At the law enforcement level, they are certainly not as embracing of technology as we happen to be here in our own country and even in parts of Asia, where one of the things that is not as apparent is the use of the Internet. You have to remember that in some countries the Internet is not even on line yet, because the Internet is controlled by military regimes not by the community and certainly not by law enforcement. That is one factor.

The other factor is the level of their economy does not allow them to get into e-commerce as we have in this country. I suspect too that there is a lot of speculation involved. If you had asked me the question two years ago—or when I sat as an assistant commissioner of crime with my fellow assistant commissioners dealing with the potential e-crime issue—I would have said to you in all honesty that I would have anticipated an exponential growth in e-crime in our country. It simply has not happened. Other countries have had similar experiences. What they have had—where they have opened up these national cyber crime centres in Europe and the United States—is a lot of referrals, but the referrals are not ones that we would deal with on a regular basis in our own country. A lot of it is because of the gap between what the private sector is providing and what the public sector is providing.

I think there is a real threshold question here, that is: how much should the private sector provide? If the private sector is producing this technology to reduce its bottom line, then to what degree should the private sector protect that investment? What we have found is that this anal-

ogy could be used as an example. It is like leaving jewellery on the bedside table, leaving the curtains open and the window open and the door unlocked and then complaining that the jewellery got stolen. There needs to be a move by the private sector to work in partnership with the public sector.

We made an approach through the CEO circle last year to have two forums—one in Melbourne and one in Sydney. We wrote to every CEO of every private sector agency in this country inviting them to each of those forums. The response was pitiful. The response was great from the public sector but minimal from the private sector. At the end of the day, it is the private sector introducing this technology to reduce their bottom line. A lot of the publicity that is given to hackings and cyber attacks has generally been protection of shareholder interest because someone has not protected their ISP or someone has provided information they would not have provided in a public forum. So, as Mr Williamson was saying, whilst there is a lot of hype about all of this, you have got to come back to the nitty-gritty. The nitty-gritty is that there is very little empirical data to say that we are experiencing the exponential growth that we predicted two years ago.

CHAIR—Last week we heard from a representative of the Internet Industry Association. Have you read her evidence?

Secretary—It has not been published.

CHAIR—When it gets published, the secretary will make sure you get a copy, because I would be interested in your response to some of the things that that lady said. I do not want to oversimplify it, but in essence her line was that there was good cooperation between the industry and the police and the ISPs and so on. If you ask for information and access to things, they respond well and very much run a very strong line against any legislation requiring them to keep more records and so on. I would just be interested in your comment about your experience if people are using the Internet to pursue criminal activity. Do you get adequate cooperation from the ISPs?

Mr Keelty—Mr Williamson might have some detail of actual cases. But based on the briefings that I have had on the major operations that we have had, the answer to that is yes. We have had good cooperation where we have needed to locate an ISP and then isolate it whilst an investigation was being conducted. So from my perspective I understand there is good cooperation, but Mr Williamson might have further detail on that.

Mr Williamson—I think at a general level the answer to that question is absolutely right. There is good cooperation globally, but it is a bit like the telecommunications companies—some of them are better able to handle our requests than others. So if you have a large company or a large ISP, we have a very good relationship because they have capacity to meet our needs, and we know their needs. But some of the ISPs are quite small. They have no experience in dealing with law enforcement; we have no experience in dealing with them. That is when we do run into some hiccups, one might say.

CHAIR—Would you advocate some sort of legislation or guidelines or some minimum standard be imposed on the industry? Their argument is that, if you start to impose specific re-

quirements, costs become horrendous from their point of view, apart from any issues of privacy and so on.

Mr Williamson—AGEC is already working on the issue of record keeping by ISPs. I think the parallel is really back into the communications environment, where there are cooperative industry forums with whom the AFP and other law enforcement agencies interrelate. It is through a cooperative self-regulatory approach, which has proved very effective in the telecommunications sphere and ought to prove equally as effective in the ISP sphere. Clearly our interest is in record keeping because the records actually prove the steps of the crime if one has occurred. But that does come with a commercial cost.

Senator DENMAN—Do you know how much of computer crime is organised and how much is just done because the person is looking for a challenge?

Mr Keelty—Mr Williamson might be better placed to answer that.

Mr Williamson—I think on the first point we need to talk about two types of crime. One is old crime, the conduct of which is enhanced by technology. It might be a drug importation; it might be money laundering; it might be fraud. It happened before computers; it happens now that we have computers. To that extent, one would find no greater involvement of organised criminal elements in those sorts of offences with computers as opposed to without computers. Clearly most of the serious drug importation and serious frauds are committed by organised crime groups. In the new environment, there are the crimes that did not occur before, and hacking is an example. We find that it is not so much organised criminal groups but relatively disorganised groups of people with a common interest who are banding together more so than being united by some commercial motivation. It is often an intangible benefit that people get from belonging to the group rather than necessarily an economic one.

Mr Keelty—Senator, I might add that there is obviously the well-known case of S11 and the way they were able to use the Internet to communicate far more widely than in days gone by. As Mr Williamson was saying, the type of crime is probably not too different. It is a fraud or it is sending a threatening letter in the mail or it is distributing paedophilia material. I guess the biggest threat is that groups can anonymously contact each other where they would not have been able to before and, more importantly, that such a wider group can now contact each other. When you do get something like what we saw with the S11 and the protests at the World Economic Forum last year, it would be an interesting question to see whether they would have got the response they got had the Internet not been available to them.

Senator DENMAN—Thank you.

Mr KERR—Firstly, might I say how pleasing it is to see you here as Acting Commissioner of the Australian Federal Police.

Mr Keelty—Thank you, Mr Kerr.

Mr KERR—I wanted to take you through some of the themes that you have raised because I think they are substantial ones. The first one was that you note that the exponential increase in

crimes associated with misuse of technology has not occurred. Yet in the document you referred to us earlier, it states:

> The United States Computer Security Institute surveys major corporations annually for electronic crime levels and losses. The latest survey responses show a dramatic increase in the level of offending and/or reporting rates as putting a strain on police resources.

It gives a graph and the dollar amounts and the like. Then there are a number of other matters that are highlighted in the boxes that basically show that this is a significant and quite substantially growing area. So I just wanted to try to reconcile those two seemingly inconsistent sorts of comments.

Mr Keelty—It is a good question. I will just take you through what the AFP has experienced in the last financial year, and then I will come back to the material that is covered in the strategy paper. In the last financial year we had 150 referrals of electronic and telecommunications crime. These are matters involving criminal manipulation of electronic or telecommunications services, which could include hacking or unauthorised access. There have been 11 referrals of e-commerce.

There are two factors there. One is a definitional factor, and this goes back to Mr Williamson's earlier point about the upskilling that we are about to do in the AFP to basic, intermediate and expert level. As Mr Williamson pointed out, at the expert level we may outsource and we may retain some internal services. To that growth in the United States, if you look at the figures—and I think AusCERT produced similar figures in Australia—they say nothing about quality. So there is nothing there about what it is that was required beyond the report.

Perhaps I will draw an analogy for you. Sometimes when you open a police station in an area, you will suddenly get a number of reports of crime that were not being received before. If you introduce a program like Neighbourhood Watch, suddenly the reports of crime grow enormously because people's activity levels and awareness levels are raised. It does not necessarily mean that there is more crime. Given the embryonic stage we are at with this—and that is related to the comments I made to the chairman earlier—all the predictions a couple of years ago were that we would have enormous growth in this. We have not had growth in the quantity.

Mr Williamson—Fairfax newspapers on 27 March reported on network attacks. The headline reads 'More than 220 network attacks were launched from Australia in the week'. The first point is that what you define as a network attack does not necessarily amount to a crime. Some of these things which are 'network attacks' are actually the equivalent to someone driving down the street in a car and seeing who has left their front door open. You then need to put that parallel to what were the rest of the world's figures—that was out of 152,000 such events occurring in a week. So there are two points. The first point is that Australia does not seem to have a problem on the size, as there may be in other jurisdictions. The second point is that there is a real definitional issue of what is a crime and what is not.

Mr KERR—It strikes me as hypothetically possible, and I put it no more than that, that criminals are much in the same situation as you are—that the broad spread of technological know-how has not yet advanced to such a stage that it is routine that criminals use this technol-

ogy to implement gain making in that environment. It strikes me with a sense of assurance that this is not growing exponentially and does run counter to this document. Certainly it runs counter to what I was given to understand that other jurisdictions are experiencing. The United States, in particular, have set up the critical infrastructure program because of their concerns of national security weaknesses that would flow not just from a tax on public institutions but private institutions as well.

When I discussed this with certain other organisations, they said that we are at a very low level of preparedness for similar kinds of threats were they to emerge in this country. In each incidence they say, 'Look, when large corporations or anybody else addresses their technology weaknesses, they are usually surprised by the degree of access that is available to unauthorised users.' I am just wondering whether in that framework there is a slight degree of complacency in saying, 'Well, it's not happening here.' Perhaps some of it is simply that it is not being reported because people do not know about it.

Mr Keelty—The first comment I have to make is that I do not think we are being complacent. I guess we are just telling it as it is, as we see it. As we pointed out, we will be upskilling the entire 2,800 staff of the AFP because we believe very strongly in this and believe very strongly in the preparedness that we have to have for this. We have taken a key role in AGEC and, in fact, chaired the steering committee of police commissioners driving this. It was the AFP in the position of the chair that tried to engage the CEO circle. We are doing everything within our capability to try to work together on this and be prepared for it. At the same time I think what we have to do, without pouring cold water on it, is just take a good sober look at what is happening. The figures that Mr Williamson just read out show it, and the figures that I have just read out show it—that we are just not experiencing the growth that we thought we would.

Your other point is a good one. I think this is analogous to the level of fraud in the community. We know that if there has been exponential growth it has been in the growth of the private policing industry and, say, the big four. If you look at where the big four are engaged by the private sector, more often than not it is to identify a fraud within a company that never results in a prosecution. More often than not, it results in a dismissal of an employee and no-one ever hears any more about it.

I think there is an issue there that we certainly do not know the level of fraud committed within our community. There may be good reasons for that. It might be to protect shareholder interest or it might be to operate in a competitive market, but the analogy is there. The fact is that we do not know the level of fraud in our community that is committed, whether it be through technical means or whether it is just committed by other means. We simply do not know and we are not likely to know it because it is protected. It gets back to the chairman's point about self-regulation. You could argue that self-regulation does not work, but I think there is another reason why we are not seeing a lot of this—it is being held in house.

Mr KERR—You raised what you said to be a threshold question: how much should the private sector provide? I guess there is a philosophical issue that is subsumed by that, that is: to what extent can the public sector walk away from the provision of law enforcement in areas where large corporations and others can in a sense buy themselves out of the need for public provision of law enforcement services? How much can you walk away from this without un-

dermining the kind of bottom line of confidence that we ought to have in the way in which our society operates?

A recent good example is HIH. I do not know whether there was any wickedness or wrongdoing there. There were questions about whether directors traded whilst insolvent—all those sorts of things will emerge later. I do not know whether the regulator acted wisely or unwisely in allowing it to continue to trade after it had reports. But the idea that one can leave it to these large corporations to do as they please, and then we as a society cop the consequences at the end of the day, is not one I am particularly comfortable with. I am not comfortable with the expansion of private policing. I am not comfortable with the idea that large areas of fortresses in our cities are being patrolled by private security and not by law enforcement personnel who are directly accountable. I am not comfortable with that direction at all. I am a little uncomfortable with the paradigm that you say, 'Well, this is something that private sector operators have to be accountable for and we cannot fill those gaps.' I understand what you are saying—that if people leave their windows open and get things stolen, they are partly to blame in some sense—but I am a little uncomfortable at the larger direction that is emerging.

Mr Keelty—I think we are violently agreeing here in a sense. What I was saying is that there is a threshold level that needs to be resolved; that is, if the private sector wants to continue to operate down the technical line, then what I am looking at is prevention rather than a cure. I am not saying that the police agencies ought to walk away from this at all. What I am asking is: to what degree do you allow the private sector to continue to operate without the proper security in place? I guess you have to ask yourself: who are the victims of crime here? Is it the average punter who is using the Internet to purchase goods because it is new technology and it saves time? If you think about it, it is a great advancement for the elderly who then do not have to travel to the shopping centre. They can do their shopping without feeling like they are going to lose more money than what they should be paying to get their goods. But they are not the people we are hearing from. The people we are hearing from are the people who complain about their site being hacked. When you look at their site, you find it is not being hacked, it is just that they have not had the proper firewalls in place.

I guess denial of service is an issue in a competitive market. Suddenly we have a new way to operate our business. Because that business is operating in a competitive environment, one person is always going to try to get more of the market share than another; therefore, denial of service occurs. That is where you would think that we would be able to come in, or a regulatory agency would be able to come in, and say, 'Well, hang on, we want a fair and equitable system here for all.' I am not saying that the police agency should walk away from this. I am saying that there needs to be further engagement of the private sector. If they want to produce and use this technology—which at the end of the day is why they are closing banks down in country areas, because they do not need banks in country areas—if that is the way they want to go, that is not for me to judge as a police officer, I do not want them then to complain that their new system of operating is vulnerable. If they are going to take that step, then I am looking at prevention rather than cure. I am saying, 'Well, if you are going to take that step, make sure it provides all the security that you would have had had you had a bank operating with a guard standing out the front and people being able to come to and from the bank.'

Mr KERR—I want to ask a couple of questions that flow from this three-tier system that Mr Williamson mentioned. You indicated that on level 1 you are going to skill all AFP agents to a level of familiarity with basic computer information systems. Is that correct?

Mr Williamson—I think it goes a little bit further than that. It is actually to enable them to deal with electronic sources of evidence. If they go into a suspect's house and search the house, they can just as effectively search the suspect's computer as they can search the safe that is there. So the means becomes irrelevant.

Mr KERR—Then there was level 2. You said these would be the equivalent of your fingerprint people and involved in forensics.

Mr Williamson—That is correct.

Mr KERR—How many people would you have within the AFP now that are effectively at that second level?

Mr Williamson—They are our electronic evidence teams. We have a team in Brisbane, a team in Sydney, a team in Melbourne, a team in Perth and a team in Canberra. We find that teams between about one and four people in those locations are sufficient to meet our current demands. For instance, there is a difference in the work that would be there. The average investigator would be able to search most computers but, if an offender or suspect had taken some particular steps to conceal it or did something with the equipment so that you could not easily retrieve it, we would need a higher level of expertise.

Mr KERR—It was reported to me that there would be about 12 people who would be in that level. Is that right?

Mr Williamson—Yes, we would be comfortable with that as an estimate.

Mr KERR—Then at level 3, which is essentially systems expertise, you say that you do not yet conceptualise a case for that being retained within the AFP?

Mr Williamson—No, because the level of expertise is at such a high level, and there are many of those areas of expertise. Each operating system, each type of commercial application, is at a very high level. To maintain expertise you need continued work. Therefore, the people who have that continued work are the actual people out in the workplace who are right up to date, keeping their skills current. We would like to co-opt them, contract them, as the case may be. Alternatively, the other sources may be people in universities or other research centres at the cutting edge. When we need that at the cutting edge, that is where we are going to go. There are some areas where we know that we will forever need people at the cutting edge, and we will maintain those. In areas like cryptography, we will have our cryptographic capacity. We have one at the moment. We will keep on having one because we are going to continue to come across that as an issue.

Mr KERR—This is something which obviously needs some reflection. I appreciate that, if you wanted somebody with the highest level of technological competency in some particular operating system, keeping whole teams of those people in different sections in the AFP might

not be appropriate. But at the strategic decision making end, how many people would you say have high level competency in the way in which technology is evolving and a capacity to cut it with the sort of people that have come before us and said, 'Look, when we deal with the AFP, they don't really understand what they're talking about'? There were those remarks about the AFP's cooperation with the ISP providers, but they also said, 'Look, hang on, it's really difficult because whenever we have dealings with the AFP they don't really understand what we're on about.'

Mr Williamson—That is a problem we get in a number of areas because we have an organisation made up of individuals, and some of them perform well and some do not. What we have in terms of electronic crime, though, is an incident analysis and response team located in our headquarters. If a matter comes to the AFP through its normal channels and it is complex and needs some high level of understanding, the contact will be made with that team in our headquarters—whether the person is in Perth or Brisbane or wherever—who do have that high level of understanding. You are right in saying that a lot of our people in our local offices have that base level understanding, and that is why we have a backstop arrangement.

Ms Fagan—Our experience in discussing these issues with ISPs is where they have a law enforcement liaison unit in place. That actually helps and enhances the relationship as well. It is a two-way street when that sort of comment comes up, that they are appropriately able to communicate with us and our investigators.

Mr KERR—You can argue whether 12 is sufficient and all those sorts of things, but it seems to me that what you are going to end up with is a broad base of obviously highly well trained agents. These agents you have now are people whom I have the highest regard for. I know most of them have had substantial training and you will give them more in this area. You have a small group of people who are your forensic experts, but under this scenario you do not have anybody whom you conceptualise as being there on assistant commissioner level or something of that nature, with some strategic vision of the way in which the electronic environment is to be addressed. I do not know whether that is wrong. Maybe Mr Williamson is that person.

Mr Keelty—He is that, yes.

Mr KERR—What I am saying is, at least what you are telling us says that there is this very strange shaped pyramid. It is big, flat at the bottom, very tiny at the next level and then there is nobody at the top.

Ms Fagan—That was deliberate with the federal agents—there needed to be a bottom up. I think you can appreciate that. This skilling in IT had to occur at the federal agent level, and the reform program was very much about that. Mr Williamson runs, and is responsible as our expert, with federal agent skills as well and it is important that you have a match. Our priority is investigation as well, and then being able to touch on specialists where we need to. That is what I would offer there.

Mr Keelty—Remembering that the organisation also has its own IT areas, and we do not separate the areas. Gordon would not hesitate to go to our director of IT to talk through the issues, or even go to other areas within the public or private sector. I think the skill redundancy is a real issue here. I think Mr Williamson's point is a very good one; that is, that in order to keep

someone at the cutting edge, our experience at the moment—and we are not saying this will not change, because we will grow this expertise as the case grows itself—is that we are meeting current levels of demand and we are doing things now to improve on that situation. It may even change. If we were sitting here in five years time, we might say, 'Well, the bit at the top is that big and the bit at the bottom is that big,' but at the moment we are meeting demand.

CHAIR—I must say my perception would be that you will probably recruit, but certainly not retain, people who are IT professionals at the very cutting edge because they, apart from money, actually get their motivation from the development work and being at the leading edge. Whilst there may be a periodic need for that sort of knowledge in the AFP, you are not going to be able to provide that person with that sort of challenge on a daily basis and they would not stay. They are going to go somewhere where they get that development. Before I came here I worked in the IT industry and people like that, once the job became routine, always moved on.

As I say, you have a calibre of skill that understands technically and can do the job, but you have a different set of people—often very different characters—who have different techniques and they are actually the ones who do the developing and are at the leading edge and so on. They are not interested in that routine work. My perception is certainly at the moment that you are probably right to have your three levels, whether it was through upskilling or skilling your core of agents, you have to be able to do that front line stuff. You certainly need a team and that will grow, it would seem to me, depending on your demand.

What worries me is that if the perception is in other parts of the community, say the Internet Industry Association, that things are not as they should be with your people, then you have a relationship problem or an understanding problem in that sense. So I come back to my previous comments that we will make sure you get a copy of that evidence. I would like to get your response to some of the things that they said in their evidence, not just on whether you think their reflection on your ability is valid but also on some of the other issues which they raised as well. I think it would be very interesting to get a specific response to some of those points.

Mr SCHULTZ—The PJC has taken evidence from Vicpol about the Victorian Surveillance Devices Act 1999 as a positive model for reform of state laws in that area. You are probably aware the act extends the provisions of the earlier Listening Devices Act to cover the use of optical surveillance devices like videos, tracking devices and devices that can monitor computer transmissions. The problems at the New South Wales border were discussed at length at that hearing. My first question is: can the AFP discuss the practical implications for law enforcement in general, and in particular for the AFP and NCA, of trying to operate effectively across jurisdictions with differing laws? My second question is: does the AFP support the NCA call for harmonisation of electronic surveillance devices legislation, and would this be assisted by a scheme of mutual recognition of warrants?

CHAIR—With all due respect, Mr Schultz, we want to make it a reasonably short answer because we covered this ground earlier.

Mr SCHULTZ—Sorry, my apologies for being late.

Mr Keelty—Mr Williamson might have some specific comments on the state of the legislation across the jurisdictions for you, Mr Schultz. But we are working towards

harmonisation. It is something that we discussed earlier. I have just come from a meeting of police commissioners, where we have agreed on a way forward that we will take through our Electronic Crime Steering Committee that sits under the police commissioners conference.

CHAIR—The clock marches on inexorably, so I think we are going to have to gong you there, unless there is anything critical that you think we have missed that you want to inform us about. May the statement you gave us on the PJC-NCA inquiry into the law enforcement implications of new technology be published?

Mr Williamson—That is the answers to the questions on notice, yes, they can be published.

Mr Keelty—I will undertake, Mr Chair, to get that response from the ISPs.

CHAIR—I would be most grateful. Certainly my impression was that we were not necessarily talking the same language, so I think it is important.

Mr Keelty—That might be a client service issue.

CHAIR—Thank you for appearing before the committee today.

[10.35 a.m.]

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

PYNER, Ms Nicole Ruth, Senior Lawyer, Enforcement Coordination, Australian Securities and Investments Commission

CHAIR—Welcome. We have received the ASIC submission, which has been published by the committee. I note that that submission was forwarded by Mr Joseph Longo. I assume he is now your former national director. I understand that he has gone on to the greener pastures of the private sector. Only a couple of months ago he was here at a hearing of ours in relation to the government's bill to reform the NCA Act. Certainly we were very impressed with his abilities and his expertise. He will no doubt be missed, but I would think your loss is obviously somebody else's gain.

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 any answers to specific questions be given in camera and the committee will consider any such request. Would one of you like to make an opening statement before we move to questions?

Mr Inman—Yes. I thought I might start with the briefest of comments to provide a little bit more context to the submission that we made earlier about the impact of electronic commerce on the Australian Securities and Investments Commission. As you know, the financial sector deals with information and data that are easily digitised, and this is one of the industries with the most advanced use of—and also under the heaviest influence of—IT and electronic commerce technologies in particular.

In general, ASIC has been dealing with the onset of electronic commerce from as early as 1996. We deal with it in a variety of ways. We provide market participants with information about how the rules should be applied in the new environment through our policy work. This allows industry participants to confidently plan their interests in the new environment. We help educate the public on risks and good practice so that consumers of e-commerce financial products and services can be confident that their interests are properly protected. We take enforcement action where the law is contravened and monitor others to encourage them to comply.

Lastly, it is worth stating that we are, in fact, a participant in e-commerce ourselves as the custodian of the companies database, which records the particulars of 1.2 million companies. We provide those services online, and several million transactions are effected every year. So we are obviously impacted by electronic commerce technologies in the way that we deliver those information services. That is pretty much all I wanted to say as an introduction, Mr Chair.

CHAIR—From your experience, do you believe there are sufficient tools available to you and to other agencies that you would have to work with—I assume you work with others? What do you consider to be the state of the law and the tools available generally?

Mr Inman—I think, as a general statement first, by and large the laws that we utilise and the powers that we utilise are sufficient to deal with the new economy as in the old economy. However, there are some aspects where we need to supplement, we believe, the powers that we do have specifically to deal with variations about how online investigations can be conducted, as opposed to how they were conducted in the offline environment.

CHAIR—Do you want to expand on that?

Mr Inman—For instance, a common form of conduct that we come across in our surveillance activities is false and misleading bulletin board postings in relation to securities on the Internet and the use of spam emails to affect market manipulations and pyramid schemes, for instance. We believe that a useful addition to our powers would be a provision which specifically addressed the use of spamming or chat rooms as a commercial tool in situations where the communications commercial motivations are not revealed.

The United States have had something very similar in place for many years. Their electronic distribution of newsletters is prohibited where they are used to promote securities by section 17B of the securities act 1933. The conduct addressed is 'the failure to disclose the fact that commissions, payments or some other advantage is being received from the issue of the securities for the distribution of the newsletter, and the source and the quantum of the benefit.' ASIC's view on that is that it should be no more than a civil penalty provision. We believe that the impost on business would not be great, as many cases now of conflicts of interest, or potential conflicts of interest, are addressed by honest publishers with the inclusion of disclaimers to those effects. Any burden may be balanced by the transparency of the information provided to consumers. That is one example.

CHAIR—Do you believe that the instance of some electronic crime is on the increase? You were in the audience when the previous witnesses effectively said—and I am characterising their evidence as I understood it—that really it was not on the increase as much as the popular view would have it. What is your view?

Mr Inman—We are noticing a large increase in matters. I was rationalising in my own mind what the difference might be with the evidence given by Mr Keelty. Of course I am sure that the committee has heard of one means of categorising electronic crime by the fact that it may either be an attack or the offence is represented by the use of the technology, and such things as hacking and denial of service attacks fit in with that category. The other category is where the technology itself is a means to an end—it is just a tool. By and large, we deal with the latter because, if a hacking attack or a denial of service attack is undertaken, offences are likely to be committed in relation to the various crimes acts around the country, and that is a police matter.

Where our jurisdiction comes into play is where people use the electronic commerce technologies as a tool or as a means to an end and, from our perspective, that is on the increase. Examples are where people will use the World Wide Web technologies to access a large consumer base cheaply or use false and misleading information to encourage people to purchase investments that do not exist or shares that do not warrant the purchasing of that. The same mediums are being used to promote unlicensed financial advice and to provide hot tips. Abuse of those types of technologies is on the increase. We have recorded over the last two or three

years a significant increase. That is how I rationalise it in my mind. I am sure that the AFP's course—

CHAIR—People who operate in your area are basically clever criminals and use the technology more than your average sort of keyhole thief—is that what you are saying?

Mr Inman—No. I was not trying to get that impression across. The new technologies, email and the World Wide Web in particular, have empowered market participants and consumers—investors included. They can do things now and gain access to information and make better decisions than they have ever been able to do in the past. But it has also empowered criminals. In essence, it has reduced the entry barriers to crime. People have found that those technologies lend themselves and are enticing—for instance, as a means of committing securities related frauds—because they are easy to use, ubiquitous. They provide access to many large groups of consumers and also provide anonymity to a certain degree. Those types of perceptions are, we believe, driving an uptake in the types of offences and contraventions that I mentioned earlier.

CHAIR—You also would have heard me ask the previous witness about relationships with the Internet industry, particularly relationships and practical cooperation with ISPs, and whether there is a need for legislation there or whether industry self-regulation would be adequate and so on. Could you tell us what your experience has been with ISPs when you have needed help or cooperation. What is your view on the legislation?

Mr Inman—By and large, we have found the industry to be very helpful in relation to our enforcement activities. My comments mirror those of the previous witnesses when they were saying that smaller ISPs can find it more difficult to respond to us. Often that is an education issue more than anything else. We take the time to talk to the ISPs that we have a need to deal with, explaining what our access powers are and also getting across their obligations under the various access powers.

We find that after a period of discussion even the smallest and most hesitant of ISPs are willing to contribute. So, in a general sense, I think that the industry—and the Internet service provider industry as a segment of the industry—is very helpful. We take the time to work with the Internet Industry Association, which I think you mentioned. We have various forums in which we have worked collaboratively together to benefit both their members and the law enforcement community in general.

An example of that is the production of an information sheet that explains to Internet service providers why law enforcement agencies are interested in certain types of information and explaining the access powers that exist that allow law enforcement agencies to lawfully seek that information. I also understand why Internet service providers harbour concerns about the potential for record keeping. For instance, I have been told that one of the largest Internet service providers in America can store logs in relation to an individual server amounting to several gigabytes of data in one day alone for their customer base. I think you can balance that against a number of factors.

First of all, log records lend themselves to high compression rates. I will give you an example of that. I know from experience that a heavy user of the Internet, someone who might spend 10 hours a week on it over a three-month period, would probably generate a log which involved

about 45,000 individual transactions in a log file and that would amount to about eight megabytes. Compression rates on that type of data can successfully reach between 75 and 85 per cent. If we talk about eight megabytes, that is six floppy disks at 50c each and that will come down to just in excess of one floppy disk.

If you combine that with the cost of memory media falling, in the same way that integrated circuits follow Moore's law of doubling or reducing every two years by 50 per cent, experience and history have shown that memory media follows the same path. My final comment on that would be to say that there are precedents which show that often an impost on business is necessary to ensure that the robust rule of law that we have in our Australian society is maintained. The proceeds of crime legislation provides in a number of places examples where government decided that that was the case.

Mr SCHULTZ—On the question of cost, are you aware of the views of ISPs on the retention of communication logs which they oppose on cost grounds other than when already kept for billing purposes? If they were required to retain such logs, what length of time would be appropriate, in ASIC's view? Are you aware of any difficulties experienced by finance institutions in their record retention obligations under the Proceeds of Crime Act 1987?

Mr Inman—I am not aware of the last part because ASIC per se does not administer the Proceeds of Crime Act or utilise it too often. I do not have any information on that. My comments about the logs was specifically aimed at communication logs. I will put it another way: we cannot underestimate the importance of communication logs in the investigation process. In the old economy, if we had a physical document there was tangible collateral evidence to support the investigation. You had fingerprints, you had forensic handwriting experts. When you move that document online, you lose that collateral information and the only replacement for that is communication logs. The information that provides you with the source, the path, the destination, the identity and the content of communications is vital. Without that, investigations do not proceed. There are examples that ASIC has had where we have been defeated because communication logs have been overwritten or were not turned on in the first place.

Senator DENMAN—Does ASIC think that its experience in combating computer crime is sufficiently general in value to be applicable to law enforcement agencies?

Mr Inman—For every success that ASIC has had I am aware of successes in other law enforcement agencies as well. There is no doubt that, even though the legislation that we administer differs, the commonality is the underlying technical infrastructure that represents the Internet at the moment; therefore the skills and the capabilities we have are common in certain areas.

Having said that, I must also differentiate ASIC from a lot of the models that I am sure you have heard about from other law enforcement agencies. We do not have computer forensics. We outsource that. We outsource that either to the Australian Federal Police, to our other police services or to the large accounting firms and the computer forensic capabilities that they have. However, we believe that conducting online investigations is an essential core competency for us and it is akin to following the paper trail in the former days.

We have similar training provisions to what I have heard the Australian Federal Police talk about. If I were to continue with their model of the tiers, they spoke about three tiers, which is generally the accepted model that the police services use. If I were to explain ASIC's approach, I would have to expand on that and say that we split the first tier of awareness into two and we outsource three and four. So what we have is a training program that ensures that our people, whether they deal in a policy setting or in an investigation environment, are at least aware of the underlying technologies that are represented by the Internet technology. Then they can be informed when they are making policy and also understand the complexity of any investigation that they come across.

We then supplement our investigators' knowledge with a further course which teaches them more in-depth online tracing skills. We provide them with a deeper knowledge of the Internet protocols and we also give them an introductory awareness of computer forensics to ensure that they can manage the relationship with the outsourcers. When it is time to execute a search warrant and seize any hardware or software, we then go to the outsource model, which would be tier 2 of the imaging that the AFP spoke about. We use those same outsourcers or sources of skills, depending on the complexity. With respect to tier 3 that the Australian Federal Police spoke about, we do not often come across that ourselves but we would use consultants when we do.

Senator DENMAN—In your submission you say e-money laundering is thought to be negligible for now. If there is an increase in that, are you ready to deal with that?

Mr Inman—Our comments were aimed at supporting the work of AGEC and there are other Commonwealth law enforcement agencies who have more of a mandate for money laundering than we do.

Mr SCHULTZ—On the bottom of page 4 of your submission, ASIC has commented, in relation to the committee's money laundering terms of reference, that it endorses the RGEC report. Is there any particular aspect of the RGEC report that you would encourage the JC to consider?

Mr Inman—Not having that document in front of me, I will have to talk in general terms, if I may. I think that the RGEC report recognises the importance of tripartite responsibility for e-security, and that is where consumers themselves have to be given the opportunity to become aware of the implications of trading online and the sorts of due diligence checks that they should do. I think business and industry need to understand their responsibilities for making sure that the front doors are locked and the bars on the window are appropriate. I think that government agencies need to work with both of those other partners to provide a safety net to ensure that Australia becomes one of the most secure online environments in which to do business.

To achieve that means working with industry and working with consumers, and the RGEC was right in stating that. The RGEC report also has suggested that a centre of expertise somewhere for computer forensics would be a worthwhile endeavour, and I would agree with that, too.

We have a small team within our organisation who provide our own centre of expertise. If we knew that there was another body from which we could get rapid advice, that would be significantly useful to us. I have already spoken about how ASIC believes that there are some aspects of online investigations which require some new powers, new legislation. I have mentioned one example of that. There are a number of others, and I think the RGEC report recognises that fact.

The action group into the implications of electronic commerce on law enforcement is working in committee at the moment to further those suggestions from the RGEC report. ASIC supports that work and participates. Hopefully, any of the benefits that will accrue from that work will accrue to ASIC's investigations at the same time. They are the main points, from memory, that I think are worth restating from the RGEC report.

CHAIR—You heard us talk to the previous witness about harmonisation of legislation. Is that an issue for you?

Mr Inman—We are luckier than most in that the national scheme that underpins the Corporations Law means that we are a national organisation. When an ASIC officer walks across a boundary, they are in fact still operating under the same provisions of the Corporations Law and the ASIC law. However, there are times when our investigators in various regional offices have to plan for the fact that, whilst they are in that particular jurisdiction, they have to abide by the jurisdiction—for instance, the evidence rules or the evidence acts. There are some differences for which we have to plan. But because of our national scheme law, I would say by and large we are well catered for.

The real issue about harmonisation for us is an international one. Our investigations are leading us more and more where it is essential that we have an ability to obtain evidence from overseas. An example of where lack of harmonisation can cause problems for us is that in Australia you need a licence to be an investment adviser. That is not always the case around the world. If you were investigating a matter—for instance, where a webpage is targeting Australian investors from an overseas jurisdiction and that jurisdiction does not have similar provisions—it can often be difficult for us to obtain the evidence and the timely benefit.

I would say that international harmonisation is an issue for us, but we are not still on that matter. We work with the IOSCO, which includes all the international organisations of security commissions, on several working parties that are seeking harmonisation, particularly in relation to provisions for access to information and evidence.

Mr SCHULTZ—What about at a national level? Are any state jurisdiction laws creating problems for you in that respect?

Mr Inman—Other than that we have to ensure that the evidence acts provisions in each jurisdiction are accounted for. We deal with that at the planning stage, so it does not cause a lot of problems for us. Again, it goes back to the fact that the Corporations Law is underpinned by similar acts enacted in each jurisdiction.

Mr SCHULTZ—So you lay a pathway leading up to the action that you are going to take within the national framework on a state by state basis?

Mr Inman—We do.

Mr SCHULTZ—That is good. Thank you.

CHAIR—What about the area of privacy? Obviously, you tread in some pretty sensitive areas sometimes. Does that ever cause a problem? Do you have some views on that in respect of yourselves or other bodies in terms of the new technologies?

Mr Inman—I am not sure that the public generally are aware to what extent privacy has been regulated in the Commonwealth agencies for the period that it has been. For instance, if ASIC obtains information, say, for a telephone subscriber, it can only do so in relation to certain provisions of the Telecommunications Act—section 282. Every one of those requests has to be verified by the team manager before the request is made. Those records can then be audited by the Privacy Commissioner. From time to time the Privacy Commissioner does audit ASIC to ensure that every request for a subscriber's information was obtained lawfully and appropriately. I know that all other law enforcement agencies abide by that same regime. I would say from an internal perspective that the Privacy Act has provided a safety net for privacy for Commonwealth agencies for some years now. It seems to be working well.

CHAIR—I alluded earlier to the evidence we got last week from the Internet Industry Association witness. The secretary will make sure you get a copy of that because I would be interested in your reaction to what that witness said. Similarly, there was interest, as you heard earlier, in what the AFP's reaction was, but in different areas. I am interested to know your reaction to what they had to say in that privacy area, because part of their argument was that there were major privacy concerns if legislation was passed giving access to bodies like the NCA or others to their systems.

They also went into great detail—certainly superficially, very convincing detail—about the quantum required for storage of information. I heard what you said earlier about that. I recall when I went into my first computer room, which was the size of this room, I think they had 32K of memory. We were very thrilled when we upgraded to 64K. Now I have got two megabytes on my Palm V. That is a 35-year span. So whilst I take your general point that the devices are becoming more powerful and relatively therefore cheaper on quite a quantum scale on regular levels, nevertheless, given that we are looking at the situation today—and let us say it is to cover the next five years—I would be interested to have your views on those calculations that they gave us about the cost of them having to keep the sort of records that might be appropriate.

Mr Inman—Certainly. In listening to your question, I was also prompted to include a supplementary response to the earlier questions on this. Firstly, I realise that it would be a very large impost on certain Internet service providers if it were a requirement that they keep all records forever. Having said that, I am also aware of at least one who does that. I think that if there is to be some form of obligation on Internet service providers, in determining what that length of time is, it should be determined after consultation. I am also aware of the European Council's moves in relation to record keeping. I think the last draft I saw was one billing period.

I have also attended meetings with the Internet Industry Association and its members when at least one member stated to all present that he believed maintaining log records was one means of differentiating his service from his competitors. That was because he was able to provide ex-

cellent customer service in relation to problems that customers have, because they could diagnose and trace those problems. So there are also benefits in the equation to be taken into consideration.

CHAIR—That is a good point. What about the UK? They have passed legislation recently in this area. Have you had any exposure to or experience of that? Do you have any views on it?

Mr Inman—I am aware in general terms of the RIP Act and its implications but I would not consider myself informed enough.

CHAIR—Thank you very much for attending this morning. We will make sure we send you what we talked about. The lady who appeared on behalf of that association will probably be surprised that we are asking witnesses to specifically respond. She made some very categorical statements and I think it is important that we hear the contrary view—or possibly contrary view.

Mr Inman—I agree.

[11.17 a.m.]

COWDERY, Mr Nicholas Richard QC, Director of Public Prosecutions, Office of the Director of Public Prosecutions, New South Wales

CHAIR—We have received your submission which you forwarded to us in August last year and it has been published by the committee. 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. I add that my attention has been drawn to the recent publication of your book, titled *Getting Justice Wrong: Myths, Media and Crime*. There was a particular part that caught my eye:

> Elections cause crime waves. They must; just listen to the candidates. For months before elections it becomes unsafe to leave your homes or even to stay in them. We could obviously go a long way towards reducing crime by not having elections.

At the moment I would probably not disagree with you too much when you say that we should do away with elections, from my point of view. My ALP colleagues might have much more concern than we do, in my opinion.

Senator GEORGE CAMPBELL—One of your prime ministers tried to do away with the banks a few years ago—he thought people would put their money under their beds.

CHAIR—My congratulations on the book, but we will leave the discussion on that for another day. Do you wish to make an opening statement?

Mr Cowdery—Yes, briefly. I am here principally in my capacity as the Director of Public Prosecutions for New South Wales. In that position I am concerned particularly with the proof of criminal offences and the evidentiary requirements for that purpose. I am also the immediate past co-chairman of the Human Rights Institute of the International Bar Association and I remain the human rights adviser to the Law Council of Australia. I have a very real interest in the protection of human rights as well as in the proper lawful proof of criminal offences. I hope I can represent both sides of the balance.

As you have pointed out, I made a submission on 24 August 2000. That submission identified the existence of the Listening Devices Act 1984 in New South Wales as the principal legislation under which surveillance is carried out in New South Wales—in addition, of course, to the Telecommunications (Interception) Act for the purpose of telephone communications and the like. The Listening Devices Act is confined to listening devices, which in the definitions section 3(1) means:

> Any instrument, apparatus, equipment or device capable of being used to record or listen to a private conversation simultaneously with its taking place.

In recent times subsection (1A) has been added. It states that a thing is not precluded from being a listening device merely because it is also capable of recording or transmitting visual images or recording or transmitting its own position. It should be noted that this is a provision which

allows combination devices to be included in the definition but it must still include as part of that combination a listening capacity.

There are a number of devices that are not covered by that legislation, including purely visual surveillance devices, tracking devices, and what are sometimes called signal devices or devices that enable the surveillance of computers and the like. It does not include enhancement equipment that might be used in conjunction with the recording or listening to private conversations.

On 2 July 1996, the New South Wales Attorney-General made a reference to the New South Wales Law Reform Commission, the reference being to inquire into the Listening Devices Act and matters connected with it. In May 1997, the Law Reform Commission issued Issues Paper 12, titled 'Surveillance'. It pointed out, particularly at pages 72 to 78 of that issues paper, some deficiencies in the Listening Devices Act. It referred to the matters that I have referred to, but in addition referred to the absence of provisions for the testing, repairing and maintaining of listening devices when in place and what might be called the theft of electricity to run the listening devices on. It also drew attention to a problem with the retrieval of devices, but that has now been addressed by section 16A of that act.

I understand that there is an interim report from the Law Reform Commission presently with the New South Wales Attorney-General but it has not been released. It remains confidential. I have not seen it and I am not aware of the contents of it. In addition to that—as we said in the submission—the Wood royal commission reported in May 1997, at about the same time as the issues paper was published by the Law Reform Commission. It made a number of recommendations, particularly Nos 131 to 134, which recommended legislative amendment and consultation between state and Commonwealth authorities; particularly in connection with telecommunications interception. Further, in 1999 the Drug Summit held in New South Wales recommended that attention be paid to these matters for the improved detection and prosecution of drug traffickers. The Law Reform Commission interim report remains confidential.

In the meantime law enforcement agencies have been forced to rely on inadequate procedures that presently exist in the law and to look for other devices which enable them to, in effect, achieve the same result. One of those devices is the use of the Law Enforcement (Controlled Operations) Act 1997, which is principally directed toward controlled operations—that is, illegal activity on the part of law enforcement agencies that is made lawful by compliance with that act. Police and others have been using that legislation to try to overcome the lack of specific provisions relating to visual surveillance, tracking of items and the like. That situation is recognised as unsatisfactory and it further indicates the need for urgent legislative attention to what are substantial gaps in the legislative scheme presently existing, certainly in New South Wales.

In my submission it is preferable if a national scheme can be achieved. I am no great optimist when it comes to achieving national programs for law enforcement, but that should not stop us trying. At the very least there should be complementary provisions in state and territory legislation relating to the recognition of warrants and a greater uniformity in the use of definitions. It seems to me in my submission that we should be aiming nationally for the broadest definitions that will enable all existing and foreseeable devices to be included, with the provision perhaps for further specific means to be included by way of regulation.

Procedural safeguards also need to be built into any such scheme. One way of addressing it may be to have different schemes for overt and covert surveillance. So there would be one regime applying to overt surveillance—for example, video cameras in public places, red light cameras at intersections, speed cameras on the highway and matters of that kind, although sometimes they are not too overt—and a covert regime, which again might be divided into three areas—one for law enforcement authorities that would contain particular safeguards. particular accountability mechanisms, and an appropriate degree of transparency. A second regime may apply to employers who have a legitimate interest in conducting surveillance from time to time of the workplace and employees. In New South Wales we now have the Workplace Video Surveillance Act 1998 which makes provision for that.

The third category of covert surveillance may be what is sometimes described as 'surveillance in the public interest'. That would include private investigators, journalists—including television stations and the like—and any other area, perhaps also including private premises where it is not a workplace situation but a private individual who has a particular interest in conducting surveillance of some aspect of it for some particular reason.

That is one regime that suggests itself: overt, on the one hand, where the protections and the accountability mechanisms do not need to be so stringent because, in theory, everybody knows it is happening; covert, on the other hand, divided into law enforcement agencies, employers and public interest. As I said before, it would be preferable if such schemes or any other schemes that are developed are recognised across the jurisdictions within Australia. At the very least, there should be mechanisms in place that would enable some recognition of what is done in one jurisdiction in the courts of another; because we do strike from time to time, for example, the transportation of drugs across state borders. If there is a surveillance device operating pursuant to warrant within the state and it travels out of the state, then there can be evidentiary problems when the matter subsequently comes to court.

Those are the few additional things that I would like to say in addition to the written submission that was made on 24 August last year.

CHAIR—Thank you very much. I agree with you about the openness of some of those cameras. You have just categorised for us the open and the covert surveillance options. I was interested in your suggestion that perhaps in the public interest you would include the media. I wondered whether you might expand on that. The reason I asked the question was that, with respect to the other areas of public interest that you talked about, I would suggest there are restraints on what is done with that information. Whereas quite often it seems to me that the media, whilst there are obviously legal restraints, can do quite a lot of damage to an individual by publishing or perhaps subsequently retracting or apologising or whatever. It seems to me that there are not the same restraints on the media in what they do with that information that there might be on the police or government bodies and so on. I wondered whether you might like to amplify on that.

Mr Cowdery—Certainly. The media example comes to mind particularly because in the last couple of years I have had three situations where a television station has had its journalists conduct interviews with people who were subject to either, or both, audio and video surveillance. They have done it, I am sure, with the best of motives in addition to the story value that it might have; in circumstances where there either has been or there is a continuing

investigation by law enforcement authorities. So they have obviously seen themselves as supplementing the lawful activities of law enforcement.

The matters have come to me for consideration as to whether or not the people involved in that surveillance should be prosecuted. I have had to look at the circumstances in which the surveillance was carried out and the use to which the product has been made, to consider the defences under the Listening Devices Act particularly—and, in that connection, particularly the defence of the surveillance being done in defence of the lawful interests of a person involved.

It may well be that people in those positions, so-called investigative journalists, may develop leads on particular unlawful activity which, for one reason or another, they do not pass on to properly constituted law enforcement agencies but pursue themselves, no doubt for the supplementary purpose of obtaining a story. It seems to me that it would be appropriate for there to be safeguards in place if they adopt that course—safeguards of the privacy of individuals involved, safeguards on the use of the material obtained as a result, and so on.

At the moment it is unregulated. It seems to me that there might be room for a special category because sometimes journalists are in the position of being able to tap into information that a formal law enforcement investigation cannot get. That is why I suggested the media. What was the other aspect of your question?

CHAIR—I commented on the speed cameras, but the main point was why you would see the media being a special category, because it seemed to me there were not any restraints and therefore you are saying you should have it because they may have access where others do not, but it would be subject to restraint. What sort of restraint would you see as being appropriate or possible?

Mr Cowdery—If the surveillance to be adopted is overt—that is, if they are going to present somebody with a camera or with a tape recorder—then I do not see the need for any legislative regime to be in place. But if it is going to be covert, as it was in the cases that I have just referred to, where there was a hidden microphone and the camera was at a distance from the subject, then it seems to me that there should be a legislative scheme in place which regulates that conduct because the privacy of the individual is being invaded. There are no controls on the use of the product that may come from that. The public has an interest in having access to information of that kind that might assist in a proper legal investigation into criminal activity. It might achieve those ends. I cannot see any reason why there should not be a provision for the obtaining of a warrant of a certain class to enable that to happen, as in the case of any other covert surveillance, but perhaps with provision for urgent warrants to be obtained in connection with that as well.

CHAIR—What about safeguards afterwards? They may get a warrant in perfectly reasonable circumstances. What about safeguards as to what happens to the material after they have got it?

Mr Cowdery—Then there would have to be reporting back on the action taken pursuant to the warrant within a certain time and in a certain form. There would have to be some provisions for the storage and the use of the product obtained. Storage should not be a problem. The use to which that material can be put might require some detailed consideration.

CHAIR—I think that is the area that worries me more than any other. If an NCA officer uses whatever devices on me, essentially there are processes will be gone through before it becomes public; the evidence in other words has got to be tested. There are not the same constraints on the media. I think that is why I wanted to explore that particular suggestion of yours.

Mr Cowdery—Perhaps there could be some sort of review of the product obtained by somebody like the ombudsman, or where there is a specific ombudsman or specific regulator attaching to the public media, that might be appropriate, too.

Senator DENMAN—In my home state of Tasmania there have been complaints recently about an overt operation in the centre of one of the cities that is using cameras, but it is mainly for break and entering in the city area. They are using volunteers to monitor those cameras. Do you see problems with that, again with respect to what happens to the videos or what sort of access those volunteers have got to the information and what they do with it?

Mr Cowdery—It does seem unusual.

Senator DENMAN—Yes. It has caused quite a furore, I can assure you.

CHAIR—If you have an English background it is a pretty mammoth understatement, I would have thought.

Senator DENMAN—The reason given is that the numbers of police have dropped—all that sort of usual stuff.

Mr Cowdery—The only controls over the volunteers that would exist probably would be contractual—by agreement. There must be some sort of agreement that they enter into before they undertake that task.

Senator DENMAN—One would hope so.

Mr Cowdery—And one would hope that there would be secrecy provisions, non-publication agreements and matters of that kind attaching to that. You would really have to look at all the facts and circumstances around it, I think, to see whether or not it should be criticised. It does sound odd.

Senator DENMAN—One would also have to be aware of the volunteers they were using.

Mr Cowdery—Yes. The selection and screening of volunteers would be an important issue, too.

CHAIR—You touched on the issue of harmonisation of laws between the states and federal—

Senator DENMAN—Abolish states!

CHAIR—The chairman is on record as being in support of abolishing states, so we get around that problem. We will not get into that.

Mr Cowdery—I would be quite happy to follow that course.

CHAIR—Given the reality that we have to deal with today, you said that we should try, even though you felt that it was a difficult path to tread. I was not absolutely clear from your answer whether you felt the difficulty of the path was because of the sluggishness of the federal government in pursuing those areas or the independent positions that state governments might take. You might like to elaborate on that, particularly on some of the difficulties that that presents us with in terms of bringing successful prosecutions.

Mr Cowdery—I just bring out the broad brush and paint everybody the same, I am afraid. I think there are problems everywhere. Perhaps there is more that the Commonwealth could do to drive an agenda for harmonisation of laws between states and territories. This is something that has been identified in the meetings that we, directors of public prosecutions, hold two or three times a year.

We do our best at a practical level to try to overcome the legislative differences between jurisdictions. But we are continually frustrated in our attempts through our various attorneys-general to try to put items on the agenda of the Standing Committee of Attorneys-General for greater harmonisation of laws. Very slow progress is made in a number of areas. It only took us nearly 100 years to get road rules; that is a start. But the CrimTrac program has struck all the barriers that we are accustomed to between jurisdictions, and it is very frustrating.

We are, after all, a pretty homogenous sort of population in this country and it is silly to have different provisions applying in different geographical parts of it. I do not criticise only the Commonwealth for lack of leadership. I think the states and territories are unnecessarily protective of their turf as well. I think they see special considerations in their jurisdictions which really do not have much substance. But even within states and territories there are problems. This report of the New South Wales Law Reform Commission, to which I have referred, comes under the jurisdiction of the Attorney-General and his department in New South Wales.

Law enforcement, by and large, comes under the jurisdiction of the Minister for Police. The Minister for Police has become increasingly frustrated at the lack of action on the part of the Attorney-General's Department and, as I understand it, there is now a slanging match—that is to use slang—between the two departments within the state of New South Wales. So the conflicts and the turf wars that go on happen at every level. Even within law enforcement in New South Wales there are jealousies between the various law enforcement agencies in New South Wales: the police; the AFP to the extent that it is involved in operations in New South Wales; the New South Wales State Crime Commission; and, to an extent, the Police Integrity Commission in the investigations that it undertakes. I am dismayed by the lack of cooperation between agencies and between authorities who are, after all, supposed to be pursuing the same ends.

CHAIR—You did not mention the NCA in your list of organisations. Does that mean everybody gets on well with the NCA?

Mr Cowdery—I do not have a lot to do with the NCA because most of its prosecutions are conducted by the Commonwealth DPP, but we do have some and we do correspond with the NCA. I must say that the relationship between my office and the NCA, small though it is, is perfectly harmonious and productive. Indeed, one of my deputy senior crown prosecutors, Jim Bennett, is on secondment to the NCA as a member for three years. I was very sorry to lose him, even for three years, but I am very happy that the NCA will have the benefit of his work.

CHAIR—One of the recurring themes through this inquiry when we are looking at this area of technology—not only the fact that the criminals have got access to it but how you counteract that—has been the problem of expertise within law enforcement agencies. Have you had any exposure to that or do you have any views on that particular area?

Mr Cowdery—I have not within my own office because I rely on the expertise of others to give evidence to explain what has happened and to assist us in the conduct of prosecutions. So law enforcement authorities have to provide that expertise. I must say that so far we have not experienced any particular difficulties. If there have been things that have to be explained to prosecutors and then subsequently explained to courts, we have been able to do that. There is always a problem in retaining people who develop expertise at public expense. I know in the United States, for example, there are many people, particularly in this area of computer technology, who join one of the government agencies, train, develop a very high level of expertise and then go out into the private sector in the hope of making more money. That certainly happens there and there is no reason to think it will not happen here as well, if it is not already happening.

CHAIR—Would you see the need for a specialist sort of cyber-forensic unit that might service all of the agencies so that you have that expertise in one place?

Mr Cowdery—I think that would be very helpful and very beneficial. I think that would be an excellent thing to have. We have been trying for a very long time now to develop a national forensic science institute; failing that a state forensic science institute. They have succeeded in Victoria. We have not succeeded yet in New South Wales in developing a state institute. I think this expertise should be available in autonomous agencies established by legislation and that their services and their expertise should be available to all concerned, particularly from my point of view in the criminal justice process. Call it an independent agency, although it would not be entirely independent, so that would be able to provide experts on both sides of the record wherever there is a dispute as to issues that have arisen in this field of expertise.

CHAIR—So you think it would be worthwhile?

Mr Cowdery—I think it would be a very valuable development. The problem, as always, is one of resources. How is this to be resourced? If it were to come into existence would it be a national body administered by the Commonwealth? If so, would the Commonwealth pay for it or would the Commonwealth demand resources from the states and territories?

CHAIR—Of course.

Mr Cowdery—The states and territories might have their own views about setting up their own state or territory body, particularly large states like New South Wales and Victoria. There

are all these sorts of practical problems, but I think the ideal would be to have an institute of some kind providing this expertise. Perhaps it could be—I make my plug again—connected with other forensic sciences and put together with expertise in those other fields as well.

CHAIR—What experience or exposure, if any, have you had in terms of this type of crime with overseas bodies—international bodies?

Mr Cowdery—We have not had a great deal except in the areas of extradition and of obtaining evidence from foreign jurisdictions. In both those areas there are protocols and procedures to be followed which are administratively cumbersome. It is not my office that usually has the direct contact with the overseas agency. It is usually some other agency. I have occasionally sought the assistance of a prosecutor from another jurisdiction. For example, we had a witness to a murder from Korea who had gone back to Korea and who was refusing to come to New South Wales to testify and her evidence was very important to the conduct of the case. We had tried all sorts of avenues to encourage her to come back voluntarily to Australia because there is no provision to bring a witness back compulsorily and we were not getting very far. I contacted the Korean prosecutor directly through my connections with the International Association of Prosecutors and they were able to provide assistance which ultimately persuaded the young lady's family to allow her to come back to Sydney. She ultimately gave evidence and the accused was convicted. So occasionally we have that sort of direct contact.

With extraditions, we usually just provide advice in connection with them—whether or not the evidence available is sufficient to support the prosecution and whether or not, if the person is brought back to Australia, we will prosecute. But the police have the primary responsibility for the mechanics of it, for liaising with other law enforcement agencies and so on. There is again a chain that has to be followed with all of these international bodies because of our federal system. If I have an international problem I have to go to the state Attorney-General. The state Attorney-General goes to the Commonwealth Attorney-General. The Commonwealth Attorney-General goes to the Department of Foreign Affairs and Trade. They go to Australia's mission in the country. They then make contact with the foreign affairs people in that country who make contact with the law enforcement people in that country, who make contact with whatever it is that we are after. And then it all comes back—

Mr KERR—It is called keeping the unemployment rate down.

Mr Cowdery—It takes time, it takes effort, it is costly, it is extremely frustrating.

CHAIR—You mentioned earlier that you wear another hat and have a particular role in terms of human rights. With the advent of this new technology, it gives the people who perhaps should have the ability to have that technology—that is, the police, et cetera—access to that technology, but it gives all sorts of other people tools to perhaps do things that they could not do before. I am thinking, for example, of scanning and imagery type technology that you could use on somebody's private house to observe what is going on. Could you give us some of your views in terms of the impact of new technology generally on human rights ramifications as well as privacy ramifications?

Mr Cowdery—As it is used by law enforcement, there is a balance that needs to be struck regarding the use of new technology as it becomes available for lawful purposes, for the protec-

tion and security of the community. That is one side of the balance. The other side of the balance is the freedoms enjoyed by individual members of the community; the rights to privacy, to freedom of speech, to freedom of association and so on. I think that the individual rights can be protected if there are proper mechanisms in place which regulate the use of the technology so that that use is accountable. Not that it is open and transparent to anybody who wants to know what is going on, but that the use of it is accountable through proper channels to the public represented by parliament or by government.

It seems to me that if there are proper provisions in place about the use of the technology, the safekeeping of the product of that use and the further dissemination of that product, then we can get the balance right. But it is a balance. It is raised sometimes in the area of DNA, for example. The civil libertarians say that the acquiring of DNA records of people is a breach of their human rights. I do not agree with that as a bald statement. If the samples are taken under compulsion, then they are a breach of the person's human rights. But if that breach is justified and if there are safeguards in place about the storage of the information and the use to which it can be put, then I do not think we need to be concerned. It is no worse than fingerprints were and we have been living with fingerprint expertise and use since early last century. So it is a balancing exercise but if care is taken to get the balance right, then I do not think individuals at large need to be concerned.

CHAIR—I also wear two hats. I chair this committee and I chair the parliament's human rights committee.

Senator DENMAN—On the DNA issue, you have no concerns about the records of that any more than the fingerprint records; is that what you are saying?

Mr Cowdery—Yes. The legislation in place, and I am looking at it from the point of view of New South Wales but I know that it is a national scheme which is being introduced through CrimTrac. Looking at it from my perspective, there is adequate provision in the legislation that guarantees that the information will be used only for the purposes for which it has been obtained, and that is to assist in resolving criminal offending.

Senator DENMAN—I will not go on to gene technology. I have a bit of a thing about that one. That one is further down the track. Have you had any input into Australia's submission to the International Organisation of Computer Evidence?

Mr Cowdery—No, none at all. I have not been consulted on that at all.

Senator DENMAN—Why not?

Mr Cowdery—It is a good question. I am often kept in the dark about developments until the very last minute. I think it again comes down to this business of people protecting their turf. I have even from time to time read in the newspaper about proposed legislation in New South Wales that is going to have a direct impact on the way in which my prosecutors conduct their prosecutions. So I do not know why there is not more open consultation with legitimately interested parties before these things happen.

CHAIR—You might be interested to know that in one of this committee's reports which went to the government we recommended that the government pursue the Standing Committee of Attorneys-General uniform control of operations legislation be enacted by the Commonwealth, states and territories in similar terms to the law enforcement act in New South Wales. The government's response is to say they agree. The government has decided to adopt an approach to enhancing drug law enforcement strategies that seeks national consistency and draws together existing disparate state and territory practices in proposed uniform Commonwealth, state and territory operations legislation in the medium term. The government sees merit in pursuing the enhancement of the Commonwealth provisions in the first instance.

Mr Cowdery—Very encouraging, yes.

CHAIR—That is very current; I only got that two or three days ago.

Mr Cowdery—That is excellent news and I hope it can be expanded to other areas as well.

CHAIR—One of the other areas that has come up during this inquiry has been concern from some sectors, particularly the commercial sector, about whether law enforcement agencies should have access, but also whether there is a need for commercial operations in the electronic field to keep large slabs of data, access records and so on. They articulate a concern about privacy but also very much a concern about the sheer cost and effort involved in doing that, which is not inconsiderable. Have you had any exposure to instances where it was necessary to go to ISPs, for example, in the Internet area; if so, was adequate cooperation forthcoming and was the quality of the information that was needed from the investigatory authority's point of view available?

Mr Cowdery—I am not aware of that happening yet but I can see that it probably will. The contact with ISPs would be by police or other investigators in the investigating phase of the matter. I believe that in the United Kingdom they imposed requirements on ISPs and the like, not only to keep records but also to enable communications to be examined. Not having had to confront the problem, I do not think I have really given enough time to the consideration of it. There are very serious privacy issues involved. On the other hand, used properly, there could be very great benefits for law enforcement in accessing information of that kind. I do not know for the present to what extent it is possible to go behind these communications without the particular cooperation of the service provider. I know that some information can be obtained simply from the examination of an email message, for example. There are investigators, not here that I am aware of but certainly in the United States, who do that and who follow the trail back through email messages until they, in some cases, can identify actual premises. I have not had any experience of it here so I do not really feel qualified to comment on that.

CHAIR—Thank you very much for talking to us this morning. We are most grateful. That concludes our hearing for today, which brings to a conclusion the hearings phase of the inquiry. Drafting of the committee's report can now proceed with a view to it being ready for tabling in the parliament. My estimate is that we will table it in the winter sittings. The secretary has got a slightly longer time scale in mind. It will now become a matter of will between the chairman and the secretary as to when it gets tabled. I would like to thank everybody for coming today. I declare the hearing closed.

Committee adjourned at 12.06 p.m.