COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT COMMITTEE ON THE NATIONAL CRIME AUTHORITY

Reference: Law enforcement implications of new technology

MONDAY, 6 NOVEMBER 2000

CANBERRA

BY AUTHORITY OF THE PARLIAMENT

INTERNET

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

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

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

JOINT COMMITTEE ON THE NATIONAL CRIME AUTHORITY

Monday, 6 November 2000

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

Senators and members in attendance: Senators George Campbell, Denman and Ferris and Mr Hardgrave, 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 10.02 a.m.

IRWIN, Mr Marshall Philip, Member, National Crime Authority

WHIDDETT, Mr Adrien Melville, General Manager Operations, National Crime Authority

CHAIR—I declare open this public hearing of the Parliamentary Joint Committee on the National Crime Authority in relation to its inquiry into the law enforcement implications of new technology. I welcome our witnesses for today's hearing, who are representing the National Crime Authority, Mr Marshall Irwin and Mr Adrien Whiddett. I understand, Mr Irwin, that you have only just returned from the Pacific Rim Money Laundering and Financial Crimes Conference in Vancouver, so today's hearing could not have been more timely. This is also Mr Whiddett's first meeting with the committee since his appointment as the NCA's General Manager Operations in June. Congratulations.

Mr Whiddett—Thank you.

CHAIR—I understand that you have a policing background of some 36 years, most recently as Deputy Commissioner Operations at the Australian Federal Police. I want to extend a particularly warm welcome to you.

Mr Whiddett—Thank you.

CHAIR—I am sure you will be here on many occasions in the future, as will Mr Irwin. As you know, gentlemen, the committee prefers all evidence to be given in public, but you may at any time request that your evidence, part of your evidence, or answers to specific questions be given in camera and the committee will consider any such request. We have received the authority's submission and the committee has already published it. Observers can obtain copies from the secretariat officer. Mr Irwin, I invite you to make an opening statement before we move to questions.

Mr Irwin—Thank you, Mr Chairman. Firstly, let me say that the National Crime Authority, as the independent statutory agency established with the mandate to investigate national complex organised crime that transcends jurisdictions, welcomes this opportunity given to it by the parliamentary committee to address key issues and concerns which confront law enforcement in the area of the exponential and rapid growth of new technologies.

That this is a significant issue for the Australian community, government and law enforcement is demonstrated by the recent scoping paper by the Australasian Centre for Policing Research, called *The virtual horizon: meeting the law enforcement challenges*, which is aimed at developing an Australian law enforcement strategy for dealing with electronic crime. Internationally, as the committee would be aware, the United Nations, the members of the G8, Interpol, the Commission of Europe and the OECD are all doing work in this area.

As the NCA's submission and the other submissions to this inquiry recognise, there are enormous benefits that flow from the utilisation of new technologies, including electronic commerce, both to the community, to government and law enforcement, including the

availability of the new technologies for law enforcement to use in pursuing its aims. In fact, these are the opening words of the Australasian Centre for Policing Research report that I have referred to. However, as that report recognises, as our dependency on the new technologies increases, so too does our vulnerability. As the report states:

> The abuse of computer technology may threaten national security, public safety and community wellbeing.

Organised crime, which the authority has the mandate to investigate, has the potential to exploit gaps in the current policing and law enforcement response in order to conduct illegal business and successfully launder the proceeds of crime because of the ability to anonymously and rapidly move wealth without the involvement of a third party. It has been estimated in the report that I have referred to that as much as $US5 billion is globally laundered each year.

Traditional crimes are facilitated by technological advances, and new opportunities are created for criminals. The report argues that law enforcement and government should act now and not wait for a critical disaster that will force a reactionary and somewhat late response. Law enforcement requires to be properly resourced and to have access to legislation which caters for the use of new technologies by law enforcement to enable it to respond effectively to the use of those technologies by criminals.

As you have mentioned, Mr Chairman, I have recently returned from the Pacific Rim Conference on Money Laundering and Financial Crime that was held in Vancouver, attended by representatives of some 50 different nations. During that conference, Mr James Johnson, who is the Under-Secretary for Enforcement at the US Treasury and responsible for FinCEN and US Customs, made these points in a speech at the conference: firstly, money laundering was a real threat to the security of nations, and it is something that must be seriously addressed; secondly, that when a new technological device is developed to allow the exchange of value through cyberspace, there is always a criminal trying to find a way to exploit it; thirdly, law enforcement and financial industries are key components in ensuring the security of the global economy; and, finally, it is important to address this issue correctly because a failure to do so could result in the global economy turning an undifferentiating eye to the proceeds of honest labour on the one hand and the product of criminal enterprise on the other, thereby undermining the integrity of financial institutions.

Issues such as that pose an enduring and ever-changing challenge for law enforcement and require responses to be made more quickly than has been the case in the past. It is important for law enforcement not to fall behind the game. As the Victorian police submission to this inquiry at page 53 of volume 1 that has been supplied to me states:

> There is a legitimate perception that technology that facilitates various crimes is growing at a rate that law enforcement agencies have difficulty matching.

As the Australasian Centre for Policing Research has observed in their report, any law enforcement strategy must facilitate electronic commerce and economic growth. It must assist Australia in maintaining its competitive position in the international marketplace by ensuring consumer confidence and protection and a stable national and international environment conducive to investment and engagement in economic commerce. That point is also made by the Australian Information Industry Association at page 69 of volume 1.

It is recognised that, in achieving these aims, there is a delicate balance to be struck between developing systems for prevention and control of money laundering on the one hand, without unduly restricting commercial activity on the other, and also a balance between the protection of privacy rights of citizens and the wider public interest in providing law enforcement agencies with appropriate tools to maintain law and order within the community. That last point is made in the papers that have already been provided in volume 1, both in the annexure from the Wood inquiry at page 96 and the Ombudsman's submission at page 118. I would like to say up-front, and I hope the committee recognises, that the authority has always been sensitive to privacy implications and is sensitive to the need for accountability.

Against this background, this inquiry involves, as I am sure the committee recognises, a range of complex legal, social and policy issues. The submission that the authority has already submitted raises concerns about the current patchwork of legislation, particularly in the area of electronic surveillance. It stresses the need for a uniform national legislative scheme, underpinned by an appropriately resourced cyber forensics facility or capacity. It suggests that, at the very least, the difficulties of the inconsistent legislative regimes around Australia, which have been recognised in other submissions from the New South Wales DPP, the Queensland police minister, the Victorian Police Service and the Victorian government, be addressed by at least a regime of mutual recognition of warrants and perhaps some consideration be given to enabling some of these powers to use electronic surveillance to be expressly provided to the authority in its own legislation. Any such legislation should extend, as in the case of Victorian legislation, to the ability to use computer data surveillance devices and to conduct covert computer intrusions.

The submission also recognises the need for agencies such as the NCA to have a cyber forensics capacity, as I have already mentioned, as part of the multidisciplinary approach that the authority already conducts. I note that since writing the submission the authority again has had regard to the report of the Australasian Centre for Policing Research which recognises the need for a national forensic computing capacity, but also stresses the importance of individual agencies maintaining and developing an appropriate response capacity. The submission observes, as do a number of other submissions again from the Victorian police, the Queensland police minister, the Australian Bureau of Criminal Intelligence and also the Australian Information Industry Association that there is a need for law enforcement to be able to go behind encryption techniques.

In fact, at the conference that I have already mentioned, there was a paper provided by Professor David Friedman of the University of Santa Clara in the United States. Although the particular paper I am about to refer to was not provided at the conference, it is available on his web site and it is entitled *The world of strong privacy: promises and perils of encryption*. It advances the proposition that we are moving towards a stage where, through the encryption technologies available, there can be effective privacy for the future. If the committee is interested, I can make some photocopies of that paper available, because it does demonstrate some of the problems and also some of the potential solutions for law enforcement.

CHAIR—The committee would be most appreciative.

Mr Irwin—I will make some arrangements to provide that to the committee after this hearing. The authority's submission also advances the need for greater regulation of information

service providers, particularly by requiring them to keep records. I note that theme has also been picked up in the submissions from the Western Australian police minister, the Australian Securities Investment Commission and the ABCI. The submission suggests that there could be clearer provisions for the dissemination of information and, in relation to the second term of reference, discusses the problems caused by the global and transnational nature of money laundering, as well as the anonymity provided by the new technologies that I have already referred to. It also addresses the concern that identity fraud will be enhanced by the new technologies, that online gambling can be used to facilitate money laundering and that underground banking will also be facilitated by those technologies.

It suggests the development of a civil forfeiture regime to forfeit proceeds of crime at a Commonwealth level and, indeed, in all jurisdictions in Australia. It suggests that some amendment is required to the AUSTRAC legislation to ensure that it can obtain information about financial transactions from all providers of financial services and not be limited to the current definition of cash dealers. It also stresses the importance of international cooperation in relation to the third term of reference, raising issues such as the amendment of the National Crime Authority Act to allow for international task forces to be formed, as well as national and state task forces as is currently provided, particularly in the context of problems with tax havens.

It also suggests that the Australian Taxation Office should be able to have access to telephone intercept information to make tax assessments and that there be an enhanced mutual assistance regime to allow for the real-time electronic communication of information required by the law enforcement agencies. The submission also suggests that, because of the rapid changes in technology and the effects of those changes that I have already mentioned, there does now need to be a constant monitoring, by government and committees of this nature, of the resources available to law enforcement to meet these challenges and also a need to continually monitor whether the legislation that exists is sufficient to achieve the purposes that I have mentioned, which include ensuring a safe and secure environment in which business can have confidence in carrying out its functions. Thank you, Mr Chairman, and members of the committee for the opportunity to make that opening statement.

CHAIR—Thank you, Mr Irwin. You have obviously touched on a wide range of matters that we would want to investigate in more detail. I will start off by asking about one particular issue that, because of my own working background, I take a particular interest in. You mention in the conclusion of your submission that ‘there is a need for improved regulation of ISPs to ensure a higher level of accountability and improved cooperation with law enforcement agencies’. Could you spell out in a bit more detail how you might see such a regime working?

Mr Irwin—Yes. In doing that, I could refer to some of the other submissions which have been provided to the inquiry on this issue. Perhaps the most critical submission relating to ISPs is that which has been provided by the Western Australian Minister for Police and Emergency Services at page 109 of volume 1 of the papers. He, in common with the submissions from the Australian Securities and Investment Commission at pages 48 and 49 and the ABCI at page 10 of their submission that is separate from the book—

CHAIR—You were not ready for this question, were you?

Mr Irwin—suggests that—the authority would adopt this suggestion—what is important is that the ISPs keep their records for a sufficient period of time to enable law enforcement to gain access to them, just as it gains access to call charge records from the carriers under the telecommunications act to indicate who has been talking to whom at what time, so that similar information is available in relation to those people who are using the Internet to communicate. A lot is dependent on a requirement on ISPs to assist by retaining their records for a reasonable period of time. That is not to say we do not get some cooperation from ISPs but at the moment it is entirely voluntary and, as the ABCI points out, while there may be cooperation for law enforcement from the larger Internet service providers the smaller ones do not necessarily cooperate to the same degree.

CHAIR—For that to be effective, though, wouldn't you need an international regime or set of standards, because really the people operating at this end would presumably only be part of the picture in matters that you are concerned about.

Mr Irwin—I agree with that and, although I cannot talk necessarily authoritatively about this, one of the things that we do refer to in the submission—and I think it is picked up in some of the other submissions as well—is some work that the Council of Europe is doing to prepare a draft treaty on cyber-crime. I am really only talking from an article which I read in the *Australian*, dated 31 October. It is quite possible that that article has had access to a later draft of the submission than I have seen, but I notice that one of the things that is reported there as potentially forming part of that treaty is to require ISPs to retain customer records. So that there does appear to be some international recognition amongst the 41 countries that constitute the Council of Europe of the need to retain customer records.

CHAIR—Moving on a little bit, when you talk about international cooperative arrangements amongst law enforcement agencies needing to be encouraged and supported by government through harmonisation of laws and so on, can you give us an outline of just how much work is going on on that international scene. It just seems to me that fundamental to this whole area is not just how we play in our own backyard here but is, in fact, about things going offshore and coming from offshore.

Mr Irwin—I would be interested to let Mr Whiddett talk on this issue as well. I think that at the moment the approach is largely fragmented and that is why there are agencies such as the Council of Europe that are trying to develop draft guidelines and standards to suggest that there should be harmonisation or greater consistency of laws. My observation is that there is a great deal more work that needs to be done in that area. It is something that is really only starting to be recognised at the present time. I do not know if you want to add anything to that.

Mr Whiddett—I think, particularly in Europe, law enforcement agencies cooperate fairly closely because they have to, with the collapse of a number of states in Europe and the boundaries becoming pretty much anachronisms. Sovereignty in that part of the world is, of course, under attack and law enforcement agencies have had to cooperate more closely. Therefore, the relationships in, say, the Northern Hemisphere are a little bit more sophisticated than they perhaps are elsewhere. Certainly in the United Kingdom and in the main European agencies in the United States there is a greater sense of interdependency and the need to cooperate across boundaries, but those boundaries still exist. I do know, for example, that in

relation to practical matters of extradition and the passage of information it has sped up considerably. We have to work on that in this region as well.

CHAIR—The American economy, of course, is the biggest and going like a steam train at the moment, and presumably their crime scene is doing something similar. The Americans, it would seem to me, are fundamental to any international cooperation. Is that the case? How good are the Americans at cooperating with us, with people in Asia, as well as with people in Europe?

Mr Whiddett—There is no question that under the current administration in the United States—and when I say that, I am talking about, say, in the FBI, the case of the director, Louie Free, who was in Australia last year—there is not just a sense of rhetoric but a sense of reality that they want to cooperate more with law enforcement in this region. The Americans too recognise it, particularly with the drug traffic. There is no doubt that the drug traffic has changed the whole dimensions of people's thought on this. They have to cooperate right across the globe and, again, they accept the fact that there is a high degree of interdependency. I would say that perhaps in the last 12 months to two years there has been a much closer relationship between ourselves in Australia and the Americans and Canadians over quite practical matters. That is not to say that it has not happened before but, increasingly, the target organisations are very global, very aggressive and require the full apparatus of both hemispheres.

CHAIR—But if drugs are the reason why there is so much international activity and need for international cooperation, presumably a lot of those drugs are coming out of Asia, so how is the cooperation going in Asia?

Mr Whiddett—Cooperation in Asia can be patchy, there is no question about that. It depends on the priorities of countries but, effectively, I think that there are people of goodwill in all of those countries in law enforcement and in government. We have to recognise that some of those states are disrupted to some extent and that does play into the hands of those who will exploit it, but there is no question that we have very close relationships with law enforcement in South-East Asia.

Senator GEORGE CAMPBELL—I have a couple of quick questions at this stage, because I have another meeting. I have a number of other issues that I want to raise, but we will come back to them at some other stage. The first question is in relation to the issues that have just been raised. There is a considerable body of work being done through the OECD on electronic commerce, protocols for cooperation between countries, taxation regimes, a whole range of areas, which merely focus on business type activities. To your knowledge is there any discussion, work or anything else going on through those committees that are being set up in the OECD looking at this criminal dimension of international electronic trade, or is it something that is being done totally outside of what is happening through those national trade bodies? The drug trade is important, but there is a very substantial body of criminal activity that is happening in terms of business activities and so forth and white-collar crime, et cetera.

The second question, which is something you might want to take on notice and give some thought to, Marshall—it might have been discussed at that conference you were at—is how do you deal with the question of Big Brother in this whole area of the Internet and electronic communications? If you provide some legislative basis to organisations like the National Crime

Authority to be able to access records, et cetera, for those sorts of purposes, what types of protections can you build into the process to ensure the ordinary citizen that George Orwell's vision of *Nineteen Eighty-Four* is not alive and well in the 21st century? That is a major concern.

I have been at a couple of conferences in the United States, dealing with the Internet, which were essentially about other issues, but they deteriorated into a three-hour savage debate about this issue of privacy. It is alive and well, no matter where you go, when you start talking about issues related to international electronic transactions. Those are the two issues. If you cannot answer them now, by all means take them on notice and we can come back to them.

Mr Irwin—I think I can answer the second question, personally, better than I can answer the first. We appreciate that that is a problem or at least a live issue and, as I recognised in my opening statement, there is a balance to be drawn. The National Crime Authority, speaking for itself, is not afraid of accountability. Mechanisms could be built into the process such as already exist in telecommunications interception legislation, for example, and a range of other electronic surveillance legislation, where the intrusion can only occur through the authorisation of a judge or a sufficiently qualified judicial person, and that there be some external overview of the way in which the authority or any other agency discharges those functions, for example, by extending the role of the Ombudsman or someone similar to that.

I would accept on behalf of the authority that any additional powers that agencies were given in this regard would have to be balanced by those types of accountability mechanisms. Obviously, if there were to be judicial approval or a judicial warrant, there would be strict legislative criteria that would have to be complied with before the warrant could be obtained. I cannot talk personally about the OECD. I do not know if Adrien has any knowledge about that.

Senator GEORGE CAMPBELL—In those circumstances, would you see whatever information gathering goes on being specifically targeted to the issue that is the subject of the surveillance, or do you see it having a capacity to cast a wider net? The problem is that there will be multifaceted communications going on. I suppose in this situation, if you are targeting someone for a drug-running activity, et cetera—there may be a range of other interchanges going on that pick up on someone else for doing something that is outside of the initial scope of the warrant—would you see your capacity to be able to transgress into that area or simply the information that you are after being limited to the transgression that you sought the warrant for in the first place?

Mr Irwin—My personal view would be that, in those circumstances, if some other serious criminal conduct was brought to attention by virtue of a warrant, law enforcement should be entitled to use that information. I do not see that position as greatly different from the situation that exists now with search warrants where, if you go to a premises with a search warrant to investigate a particular crime and while you are there conducting a legitimate search under the search warrant you find there is evidence that the person has committed another serious crime, you are still entitled to seize the evidence of that other crime.

Senator GEORGE CAMPBELL—The difference here is that you are not just searching property, you are searching inside people's heads as well. That is the dimension of this.

Mr Whiddett—The same applies for listening devices in telephone interception; in other words, the warrants have been taken out for a good reason and provided by a judge.

Senator GEORGE CAMPBELL—I understand that.

Mr Whiddett—But in the midst of a lot of dross there may be only a few pearls of something interesting. That is the reality at present. There would be a vast amount of material gained by that means, which has no particular interest to the matter in hand but may be of a private nature. It is a question of discerning what is valuable to law enforcement and what is not. In the first place, again, it is provided on the signature of a judicial officer; it is not law enforcement on their own frolic, as it were.

Mr Irwin—I should make it clear that, by answering the question in the way I have, law enforcement would not be interested in every bit of information that it might pick up by intercepting the Internet or computers or whatever.

Senator GEORGE CAMPBELL—I know you are not. The concern I have is that the direction in which we are going is much more pervasive than anything we have known in the past. The window of view is much wider than it has ever been in the past. That will raise very serious consideration of privacy issues.

Mr Irwin—I appreciate that. It does raise itself from time to time, as Mr Whiddett points out, with listening devices and so on. As an example, if there was a warrant that allowed interception for the purposes of investigating some drug activity or some money laundering activity and in the course of that you picked up information that there was going to be a professional assassination of somebody, whether connected with that activity or perhaps connected with some other activity, then that is the sort of thing that I envisage law enforcement would have to be able to do something about. It is like a lot of things, I think. It is a matter of where you draw the line and there would have to be some fairly clear legislative provisions about it. I cannot answer your question about the OECD off the top of my head, however.

Mr Whiddett—There are a lot of organisations looking at that and I am certain the OECD and the International Bankers Association have an interest in it; Interpol certainly has committees on this. Generally speaking, it is a very current topic.

CHAIR—Following on from Senator Campbell's questions, if you have reason to suspect somebody and you are telephone tapping, have a search warrant or you are in the environment we are now talking about going into an ISP and looking at traffic there and so on there is less the concern about whether they are engaged in some criminal activity and you happen to stumble on some other criminal activity. I do not think too many people are going to argue that, whilst you are investigating a drug thing, if you discover a plot to assassinate somebody, then that is fair game. The concern is that you would obviously as collateral damage, so to speak, pick up information that may not be illegal but which could be embarrassing or whatever. Then there comes the question of the security of that information. Could you, for the committee, elaborate on the sorts of measures that you and other agencies might take to make sure that that does not happen. We have had in the media quite a lot in recent years mention of the fact that unfortunately not all policemen, like not all politicians, are pure and people are concerned that

legitimate—nevertheless private—activities or business may in fact be exposed by the potential widespread use of these sorts of more modern devices.

Mr Irwin—Before giving Mr Whiddett the opportunity to respond to that, I personally make the point—which I am sure the committee will readily accept; I probably do not need to make it—that law enforcement does not have any interest in that sort of information and does not have any interest in trading in that sort of information. It is clearly only interested in that information which advances its investigations in the discharge of its functions. Secondly, the material within the authority is given a high classification and is treated accordingly. Thirdly, under the National Crime Authority Act, as the committee is aware, there are significant penalties for people who do leak information and, fourthly, by a form of external overview by the Ombudsman it appears likely, under the proposals that have been put forward by the government, that that will provide an independent checking mechanism to ensure that the information is being dealt with appropriately.

With telecommunications interception information, for example, I am not aware of any case where the Ombudsman has ever suggested, so far as the authority is concerned, that it has not been dealt with appropriately and with all due security being provided to it. I do not know if Mr Whiddett wants to add anything to those general observations. I should say this though: obviously any system is only as good as the people who are within it and, whether it is the authority or anybody else, law enforcement can only do all those things that are reasonable to ensure that there are no security breaches. Certainly so far as telecommunications interception legislation is concerned,to repeat myself, I am not aware of any breaches ever being found or suggested against the authority, for example.

Mr Whiddett—I can only add, now being in the authority, that was certainly my finding in recent times—the Ombudsman does review the telecommunications interception arrangements of the authority and there is a very high level of conformance with the law and the regulations. The only omissions have ever been minor clerical entries in books and so forth. There has never been a case where there has been a gross breach of duty. The other thing is that the way the authority works internally is in small teams. The ‘need to know’ principle is pretty high in the NCA as compared to, say, a conventional police agency. So a lot of information that may otherwise find its way to a variety of people in general policing does not find its way out in the NCA. There are no guarantees in all of these things, but it is, I would say, one of the tightest procedures in Australia.

CHAIR—You are effectively, as I read your submission, advocating that we need more harmonisation of laws, we need more technology and more entitlement to access ISPs and records and so on, but we also need more working together with other agencies both nationally and internationally. I put it to you that one of the dangers of that is that you are basically going to finish up with more information in a far bigger network and, therefore, whilst you can contain it in a small network at the moment, if you have a far bigger information pool and a far bigger network of people who might have access to that, then the risk is that much greater. Whilst it may be fine to say, ‘We can take some action against somebody who’s found to break the rules,’ that is little consolation to some innocent soul who has had their career or their business ruined in the process. I think it is the balance that we are probing in that sort of sense.

Mr Whiddett—I suppose I can only point to the fact that life contains a whole range of risks and with globalisation those risks will increase, not just in relation to law enforcement but to general trade and commerce and life generally; in other words, I think all of us to some extent will be a lot more exposed than we ever were to a whole range of things. But the reality is that the criminal element is not constrained by any of these mores or concerns at all, and that is something that we have to also take into account in the balance. In other words, I think that, for the purposes of the harmonising of a lot of legislation, the hour is late. We are not working as effectively in this country as we might and it seems to me, from my observations of law enforcement over a number of years in Australia, that the NCA came into being in 1984 to counter precisely the problem that we have with the fracture federally of law enforcement just in this country alone, forgetting what we might do in cooperating with foreign states. All I can say about the safeguarding of information is that it is only relevant information and proper intelligence and evidence that is provided to participating law enforcement agencies. There is no question of a system that would provide formally for the provision of salacious data that had nothing whatsoever to do with a case, but in any human system there is always room for failure.

Senator DENMAN—Just a follow-up question on that: you said that we were not working effectively in this country. Have you any idea what sort of a budget we would need to bring us up to speed? Is that the problem—it is multi?

Mr Whiddett—It is not really budget. Budget could be part of it, but if you simply select budget as an issue alone, it is not enough. I think that the real issue is the harmonisation of laws and the capacity for law enforcement to move across boundaries in this country in a way which does not put us in the same position as we are at present with foreign states.

Senator DENMAN—You are saying that from state to state it is a problem?

Mr Whiddett—Yes.

Senator DENMAN—We need to have similar laws across the borders?

Mr Whiddett—Yes, just compatible laws, so that if an offence occurs in one state it is recognised in another if the person goes there or is caught there. In this day and age, people move rapidly. Many countries of the world have overcome this problem and we have not quite overcome it here.

Senator FERRIS—We found that in our inquiry into undercover police operations.

Mr Whiddett—That is right.

Senator FERRIS—If somebody is operating in Albury, they are covered. If they go across a bridge and are in Wodonga, then they are not, in the legal sense. Can I ask a question about resources. It often intrigues me—and you have certainly detailed it in your submission here in a way that focuses me on it—how you work out, these days, how you divide your police resources into community policing, crime prevention, some of this new emerging technology, and all of the other things that go with the criminal element dimension of policing.

In your submission you talk about Brendan Abbott and the amount of stuff that he had with him that was very high technology—his electronic devices and so on. You managed to eventually catch him, but it took quite a long time. How do you work out the resources that you need in a normal police operation? Quite clearly—and your submission points it out perhaps more clearly than I have thought about it in the past—this is such a rapidly emerging area of policing and the criminals are so far ahead of the game—I am not saying that they are necessarily ahead of the police, but they are ahead of the game—that the resource pressure on you to move more staff into that and away from some of the other areas must be increasing. How do you deal with that?

Mr Irwin—I think it is a global policing issue. I might hand over to my friend who has more practical experience in the area.

Mr Whiddett—Ultimately it is a matter for governments to decide what they want to do with all the range of things: policing, education and so forth. There will never be enough resources in Australia to be able to deal with every crime report. That is the reality. However, at the higher level of crime, which the NCA is involved in, the reality is that it requires a lot of patience and a lot of resources, and that is expensive. If you are investigating a simple larceny or, for that matter, a murder, it is usually fairly contained, but if you were dealing with a very open-ended, protracted case of, say, drug trafficking or some other complex investigation such as fraud, it may well be that resources go into that effort for months or years.

That sometimes is very open ended. In other words, at the time of planning you expect a certain course of events but we are not clairvoyant and therefore we cannot always be confident that people will act as we think they will act. We do not always know all of the issues that may be involved in a case, we just have small windows into things that occur. Because of that, all the paraphernalia that is required to do the job, whether it is technical, physical surveillance or other means, is highly complex, chancy on occasions and does not always provide results, but that is, unfortunately, the nature of the work. I wish I could say that all of our work was ‘an hour less ads’, as is much of the police work on television, but it is not like that. It is exceedingly time consuming, and very uncertain.

Senator FERRIS—Have you ever thought about trying to restrict the sale of some of the electronic devices and so on that Brendan Abbott had? How would he have got those? Would he have bought them over the Net? Would he have bought them overseas? Have you given any thought to trying to restrict the retail availability of these things? Does that have any part to play?

Mr Irwin—I do not know that we have. Although, obviously, licensing and regulation are certainly ways that will stop a proportion of this sort of conduct, I suspect that, whatever restrictions you imposed, someone like Brendan Abbott is likely to be able to get these things through underground sources or a black market facility and probably will have access to the sort of people with the electronic knowledge to put these things together for him.

The case that the ABCI, I think, has referred to in its submission, with Brendan Abbott, is a good demonstration of how, on the one hand, law enforcement agencies are constrained by the legal system and, obviously quite appropriately, are subject to regulation, but the people that we are trying to meet are not. Brendan Abbott has no difficulty in moving across borders with

electronic surveillance equipment. He does not have to worry about warrants and judicial approvals every time he crosses a border, whereas law enforcement agencies do.

Going back to that topic, as Adrien said, in the area of harmonisation of laws one would have thought that, with the establishment of a national body like the NCA, one of the things that was intended at the time was that here was a body that would be able to carry out policing into national criminal activity without having to worry about borders, but in fact we do. There is an issue every time someone goes into another state as to whether, under our current legislative regime, we are entitled to use some of the pieces of state legislation.

It might have been a good idea at the time that because we have AFP officers seconded to us we can use Commonwealth powers and because we have state police officers seconded to us we can use state powers, but it is not always as simple as that in practice. One of the things, of course, that does hamstring the NCA as a national agency is the absence of specific powers, subject to appropriate safeguards, that it can exercise as the NCA. I think the Brendan Abbott case really demonstrates that. The criminals have certain advantages.

CHAIR—But he got caught anyway.

Mr Irwin—He got caught.

Senator DENMAN—At an enormous cost, probably. You speak about going across borders. Do your state counterparts see that as intruding on their work? Is that one of the problems?

Mr Irwin—That is not the way I see it. Adrien has probably had a lot more experience in law enforcement than I have and has probably seen it evolve over a period of time, largely because the work that the authority does is done through task forces that it coordinates, whether it be the Swordfish Task Force, the Freshnet Task Force or the Blade Task Force. Frequently the states see the authority as value adding to their investigations. Quite often, because we do have that nationwide ability, although subject to some of the restrictions that I have mentioned, they see us as being able to help them out in investigations where they may not be able to carry them out themselves. I do not see a lot of resistance there, but I do think it is one of those things that has grown up with Federation and state sovereignty over the years that different states are going to look at things in different ways, and they find it very hard to move away from that.

CHAIR—Yes. But on that point, isn't it a fact that one of the reasons it has been so difficult to get harmonisation of laws across the country has been turf battles? This committee produced a substantial report in the last parliament and is still waiting for the government response. Part of the reason we have not had the government response, as I understand it, is that it is trying to progress the action it wants to take as a result of our recommendations through the state police ministers committee and it is taking an awfully long time. One can only assume that is because of turf wars. Would you prefer not to comment? You are going into the diplomatic corps?

Mr Irwin—I might partially. Whether you call it turf wars or not, there is no doubt that the different states look at things in different ways, taking into account their own experiences. But that does create difficulties for agencies like the authority that might have to deal with, say, a public interest monitor in one state and not in another. You might find that because one set of legislation does not have a public interest monitor associated with it in New South Wales,

Queensland might be reticent in recognising it. I am only talking hypothetically, of course, but these are the sorts of issues that do crop up and they do create significant problems for us as an investigative agency. We are able to achieve a lot notwithstanding those problems, but it would certainly be much better if we could find some sort of regime—whether it is by giving us powers under our own legislation or a proper regime of mutual recognition of warrants, of which there is some glimmer in the Queensland Controlled Operations legislation. We need something. Adrien may want to comment, based on his extensive experience in policing.

Mr Whiddett—I think lack of cooperation gets down to individuals, but the commissioners are certainly more in accord than they have ever been on cooperation. It gets down to the efficacy of the laws. If the laws are not compatible in jurisdictions, it is difficult for them to cooperate as they might. With the NCA moving across boundaries, that is not done just at a whim; it is done through the task force arrangements, and courtesy and communication are the two things you must have at the forefront of your mind at all times. You do nothing without those two things. The reality is that if people do have that view, at whatever level, it is exceedingly short-sighted for this country.

Mr SCHULTZ—I like the word 'harmonising'. It is a new word that I have not associated with law enforcement before. I understand what it is all about, and you are absolutely right: you need to have a situation where the laws of this land are compatible so that law enforcement agencies can act. I am also aware of the fact that in today's day and age you need to have access to electronic equipment to overcome the problems that are being put upon law enforcement agencies by the ability of organised crime to have access to and to use that sort of equipment to avoid detection. I am also very much aware that if harmonising of laws is going to be successful you have to have an absolute commitment by the state authorities to working with you. I am not so sure that is going to occur, because they cannot even adhere to their own laws in terms of their own penalties with their own people within their own ranks who are involved in unlawful activities, so I think that is going to be a problem you are going to have to deal with. I have had some personal experience with those sorts of issues.

The other thing that is of concern to me is that, from the NCA down, right across all of our law enforcement agencies and overseeing bodies, we can talk about what we need to do to overcome the problem of organised crime in this country, but we tend to get very easily fooled about our performance out there when we read headlines that many kilos of heroin or cocaine have been seized and what a great thing it is. This is in an environment where you and I know that the criminals involved in organised crime were forwarding two-kilo packs of heroin through the mail in the past and are now forwarding 100-kilo packs. So we have 100 times more illegal contraband coming into this country than we have had before, in an environment where we are underresourced in equipment and manpower to handle that sort of pressure.

How do you overcome those problems on the issue of harmonising and trying to get the states and indeed the AFP involved through the federal government in an exercise where they have adequate resources to assist you in the positive outcome that you are trying to achieve and the direction that you are proposing?

Mr Whiddett—As I said earlier, we will never have all the resources that we need to investigate all the crimes that are committed. Take, for example, the drug traffic. One of the things that globalisation has brought—and it is a good thing for Australia, obviously—is

increased commerce. The number of containers that enter Australia is increasing exponentially. The reality is that, without intelligence as to what each and every container that comes to this country contains, large quantities of drugs will continue to get through. We have to be practical about this. There is only so much that can be done. Customs will give you advice on the percentage of containers they can physically search, but I think you will find it is exceedingly low, given the volume.

If we imagine, as a recent report seemed to suggest in 1997, the heroin project, that the usage of heroin in Australia could be somewhere in the region of five or six tonnes annually, then that says the country is facing a significant crisis; there is no question about that. And it will continue apace. The drug problem is a major thing for this country. It is a major problem for the world. Therefore, my own personal view is that there will be difficulty containing that, no matter what resources we are speaking about. What needs to be done is greater cooperation between law enforcement, greater recognition that there is a need to harmonise the laws and a greater emphasis on intelligence. But the cooperation between police of all states, whether it is in Australia or externally, is critical to the success against this traffic, and that really is the major issue. It is more of a concern that it is very pervasive, exceedingly aggressive and involves a very high state of entrepeneurialism.

Mr Irwin—As one of us observed before, at the moment cooperation amongst law enforcement agencies is as good as it ever has been in this country, if not better. Part of that is due to the fact that over the past four or five years the National Crime Authority, rather than putting itself forward as a competitor with other law enforcement, has been coordinating these national task forces in the areas of heroin, tax evasion and fraud on the Commonwealth in particular, and has brought together, working very closely together, to a greater extent law enforcement officers from throughout the country and has caused regular coordination meetings where agencies do get together and exchange their information. Cooperation is proceeding as best you could expect, I think, at the present time. Certainly there is considerable cooperation and support for what the authority does from the police commissioners themselves, which is always comforting.

Mr SCHULTZ—On the issue of fraud, as an individual and as a member of parliament, I am well aware that there is more emphasis, for example, on chasing fraud against the Commonwealth for figures as low as $6,000 than there is in setting up surveillance and intelligence operations, which are very costly, which could have some real impact on the availability and supply of drugs in this country. I have real problems with that. That is one of the reasons why, at the outset, I said to you guys that I agree that you need to be resourced, in terms of the technology that is available today, to be able to do that. But so, too, do the other law enforcement agencies that you guys are going to have to work with. It is frustrating from my point of view when these issues are raised and, because of the way in which the funds or the resources are managed within the agencies themselves, they do not get the attention that they ought to. I will just make that point. I do not know whether you want to comment on that or not, but I am well aware of it and it really disturbs me.

Mr Irwin—Can I make these points. You may not be suggesting this, but certainly the authority in its investigations on fraud against the Commonwealth is not concerned with small amounts of money, of course. Frequently, the way in which we go about investigating it is that, because the people who are involved in the drug industry are also involved in significant tax

evasion and money laundering activities, we are often able to identify the people whom we should be targeting for drugs by looking at their financial affairs. Sometimes it is easier to convict them for their financial transgressions rather than for their other related drug activity. Sometimes the following of a money trail makes it more effective in investigating the drug activity itself. From the authority's point of view, it is looking at investigating only the most serious fraud against the Commonwealth—money laundering and tax evasion. Frequently it is used as a tool which will lead it to the people who are committing other sorts of serious illegal activities.

The other thing that I should mention in relation to fraud is that if the experience that I gained overseas of what is happening with law enforcement agencies, particularly in Canada, is anything to go by, it is likely that over a period of time ordinary police agencies will continually increase the threshold as to what fraud they will actually investigate. The agencies, particularly in Canada, are finding that they simply do not have the resources to investigate all fraud, and I think that is being found in Australia at state law enforcement levels as well. Various thresholds are being imposed, below which the frauds will not be investigated by fraud squads. I think we are going to see an increasing lifting of the game in relation to the seriousness of the frauds that law enforcement agencies, both internationally and in this country, will be targeting. I do not know, again, if Adrien has any observations about that.

Mr SCHULTZ—I just make the point that I was not referring to the NCA when I was talking about that. I was talking about other agencies.

Mr Irwin—I appreciate that.

CHAIR—Mr Whiddett, did you want to add to that?

Mr Whiddett—The other dimension which is worth while following up—it would have come up in the Canadian context too—is that a lot of law enforcement agencies now are finding it difficult to retain a lot of the expertise that they have in the area of fraud in the investigation of complex matters. Since the private sector has discovered forensic this and that, such as forensic accounting, they tend now to be providing a lot of the assistance that law enforcement would otherwise provide. There has been a shift—not gradual, but certainly a bit of a shift—over the years to a private sector regime being involved in those sorts of investigations. The consultancies see that as a very attractive part of their work: to offer a service which has an investigative, forensic capability. That, of course, has an effect on law enforcement resources.

Mr HARDGRAVE—It might help Mr Irwin to know that I had an example a few weeks ago, highlighted in the parliament, where $600,000 seemed to be the benchmark whereby one government agency would not bother to investigate the claims of fraud against an organisation. The media did not report it but, hopefully, my public airing of the issue might get some response. It seems an extraordinary amount of money that is ignored when someone has got off with that sort of level of fraud.

CHAIR—But you are not suggesting that that was the NCA?

Mr HARDGRAVE—No, it certainly was not, but I just thought I would raise the subject, and I thought I would just offer a new benchmark which seems to have been established. I

suspect that, once we can get the jurisdictions as far as penalties and laws relating to crime sorted out, we will fix up the standard-gauge rail problem! It is a major concern, I think, for us all, since Federation next 1 January we will celebrate 100 years of inexact laws in this country.

Where is there no jurisdictional problem? You have just been to Canada and have been involved in the Pacific Rim Money Laundering and Financial Crimes Conference. Elliot Ness told us about the use of accountants to get Al Capone, and in all those FBI movies we see lots of jurisdictional problems. Is there anywhere in the world where there are no jurisdictional problems like this?

Mr Irwin—I suspect not.

Senator FERRIS—How does the United States manage it?

Mr HARDGRAVE—That was a nice supplementary, Senator!

Senator FERRIS—We are allowed to have supplementaries.

CHAIR—Mr Irwin will answer if he wishes.

Mr Irwin—They do have some national laws that they are able to police through what they call the mail fraud and the wire fraud laws, but to chase people across borders, as I understand it, they do need to have some sort of national jurisdictional basis, whether it be through a kidnapping across state borders or something of that sort. Again, Adrien has probably had some direct experience in the United States.

Mr Whiddett—There are problems there too but, at least at the federal level, the US federal government in its own right has quite an array of criminal laws that it can apply. In Australia the Commonwealth does not have that sort of an array of laws; they mainly fall into the states. That is another issue which makes us slightly different from the United States. We are relying very much on the large body of criminal law sitting with the state and territory jurisdictions and a very small rump of the criminal law sitting with the Commonwealth. That is not the case federally in the United States.

Mr HARDGRAVE—Perhaps we need to break down this turfdom concept. It is a bit like the industrial relations laws which I do not expect you to be an expert on obviously; I do not know anybody who is, apart from the minister. I suspect that there is a federal award and a state award level. Perhaps we need to have federal laws and state laws so that if somebody does not get pinched adequately well on the state basis, they could perhaps get pinched on a federal basis. Is that basically what they do in the US? I am not telling you to advocate a change to the Criminal Code but I am just, as a discussion, going down this path.

Mr Irwin—All I can say is that, from the point of view of the National Crime Authority as a national body, it would be in a strong position if constitutionally it was possible to enact national laws—for example, national drug trafficking laws or national money laundering laws—which could transgress state borders. The authority would then be able to hang its investigative activities off those, but that is not the way that the system is at the present time.

CHAIR—We were talking earlier on about the need for some harmonisation because of the difficulties of operating in different states. I suppose it is the time that one should ask the question. In your submission you talk, I think approvingly, about the introduction in the UK of the Regulation of Investigatory Powers Act 2000 which, as I understand it, is an act which not only codified almost all existing investigatory powers, including covert and controlled operations, but also extended them by, for example, permitting law enforcement to demand access to encrypted data and so on. Clearly, we do not have the same structure as they do in the UK, given that we are a federal system. The UK has increasingly had devolution of political power into Scotland, and a bit to Wales. It is a different regime in Northern Ireland and so on. They presumably have some differences within the UK, so is that a potential model for us to look at in this country?

Mr Irwin—I think the answer can be given in one word, and that is 'yes'. It certainly goes a lot further than the laws do in Australia at the present time. Clearly, as the submission says, there is the need for consistent laws across the country. Whether that is done by one national law which is accepted by all or whether it is done by all states at the same time enacting some sort of mirror legislation is probably a policy issue, but certainly the sorts of things that are covered by the UK legislation and the fact that it effectively codifies these things for the whole of the country is something which would be extremely desirable in this country. It would be easier for everybody, however we did it, if we effectively had codified law enforcement powers around the nation, rather than this patchwork of different powers and different jurisdictions. And that creates problems, not only obviously for the NCA but for any state agency if it has a criminal it is pursuing across state borders.

Senator DENMAN—I have some questions here from Duncan Kerr. He apologises, but he had to go. I think I can read his writing, with the help of Senator Ferris. How many Australian law enforcement personnel have high level computer training as in the NCA and the AFP? Has this ebbed and flowed? What are the high and low points in staff with this expertise and are there enough?

Mr Whiddett—I will have to take the actual numbers on notice. The reality is that the National Crime Authority has a fairly modest capability. It depends on what is really meant by 'computer knowledge'. Having people who understand what they need to do when they arrive at, say, a crime scene which might involve technology is one issue. Then there are the people who are able to do, if you like, clever things with proprietary systems.

Senator DENMAN—I think that is probably what he means.

Mr Whiddett—They fall into very few. Some of the skills that are required in that area are not possessed by law enforcement. They are possessed by other agencies, which I do not want to go into.

Senator FERRIS—Such as AUSTRAC?

Mr Whiddett—No, not AUSTRAC.

Senator DENMAN—The next question is, how can we train and retain them in the law enforcement area?

Mr Whiddett—That is deeply problematical. The fact of the matter is, as I said earlier, that a lot of private sector agencies are paying very large sums of money to attract talent from the public sector and that is an ever present threat. It is true to say that certainly at the Commonwealth level—and no doubt at the state, too—there is a reasonable level of drainage of talent into those areas. The actual skill base is, I think, not that high across policing in Australia.

Mr SCHULTZ—There are a lot of academics but not much practical policing expertise left in the police forces today because of that process.

Mr Irwin—From my most recent experience, that seemed to be also the song that people were singing in Canada as well. It is a problem universally. One of the solutions that was being suggested in Canada was for a closer partnership between law enforcement and private industry, although for an agency like the National Crime Authority there is a limit to the extent that you can go down that track because of the confidentiality requirements. But certainly from more traditional law enforcement agencies the conference in Canada, in fact, resolved that the partnership between private industry and policing was something that had to be pursued more closely.

Senator DENMAN—His last question is, what kind of arrangements are in place to allow Australian law enforcement personnel to job swap with overseas counterparts? What, if any, examples exist of this happening?

Mr Whiddett—Again, it is not a huge exchange, but there are exchanges between law enforcement agencies and police forces abroad, both at the federal and state level, for training and some specialist expertise. It varies from jurisdiction to jurisdiction. Some organisations run courses which are purely for foreign service people—that is to do with liaison and encouraging cooperation—and there are also a number of fora that law enforcement attend which provides, if you like, enhanced knowledge on technical expertise and developments in technological areas. Australia is party to that environment. They are good things because it enables the different people—engineers, technicians and investigators—to get a sense of what developments are occurring elsewhere. It is not a large cadre of people moving all the time but certainly hand-picked people from organisations do mix. There are occasions where there is interchange between agencies. Someone may stay there for six months, 12 months, or longer.

Mr SCHULTZ—The Wood royal commission made a number of recommendations in its 1997 report for reform of the Telecommunications (Interception) Act. The government has since reviewed the operations of the act and made a number of amendments, yet the New South Wales DPP, Nicolas Cowdrey QC, suggested in his submission that these amendments have not gone far enough. Justice Wood had also recommended that the Commonwealth should devolve appropriate legislative and administrative responsibility for telephone intercepts to the states. Before you comment on that, I have grave fears about that, because Justice Wood, after that very costly inquiry that he headed, made some recommendations about cleaning up corruption in the New South Wales police force and nothing has changed; corruption is just as endemic today as it was in 1997. Do you have any comments with regard to Nicolas Cowdrey QC's suggestion in his submission that the Commonwealth should devolve appropriate legislative and administrative responsibility for telephone intercepts to the states?

Mr Irwin—My own view is that the system at the present time works reasonably well and a state can have the powers that it needs, provided it has mirror legislation to the Commonwealth legislation. I think with the exception of Queensland—I believe Tasmania either has or is about to obtain telephone intercept legislation—the system to me seems to work reasonably well by the Commonwealth legislation virtually being applied in the states. But there are some other aspects of the recommendations that Justice Wood made in relation to telephone interception that are supported by Mr Cowdrey that I am perhaps a little more interested in. They include at paragraph 1.31, at page 95 of volume 1 of the submissions, the last two points:

> There be an effective and workable regime for the continuous monitoring of advances in technology that can prevent their introduction until suitable capacity for intervention is established and ensures a timely and proper amendment to meet any such advance and current needs and also a re-examination of the current funding model with a view to requiring carriers, as part of their licence conditions, to provide at their own cost interception capability or telecommunications services which they may wish to introduce.

In relation to the latter point, I think from reading the report itself, which is also included in the submission, what Justice Wood had in mind was that, rather than the carriers charging law enforcement agencies for capital cost of making their systems interceptible, there be some minimum fee set which would be paid to carriers. That is at paragraph 7.97 on page 99. What attracts me to those two recommendations is that that may well be the sort of thing we should be looking at in relation to being able to deal with advances in technologies, such as encryption, for example. It may be that law enforcement should be given the opportunity to consider those pieces of technology before they are actually applied and that the people who are providing them are required, before doing so, to make their systems interceptible, to use a general word, by law enforcement agencies.

Mr HARDGRAVE—It is theoretically possible, though, isn't it, to be able to pick up on a URL and home in on that site and see what goes in and goes out? By its very nature, the Internet is a party line and pretty open.

Mr Irwin—It is at the moment, but there is the question of encryption for the future, and that is probably the thing that concerns me more. It is one thing to intercept the Internet at the present time in an appropriate case but, as time goes on, there are going to be stronger and stronger encryption services available. That is one of things that the paper from Professor Friedman talks about. He almost seems to be advocating it, and I would not agree with that; nonetheless, we are moving to a world where there will be a significant degree of privacy of communications unless law enforcement is able to get behind them in an appropriate case with appropriate safeguards.

Mr HARDGRAVE—Are all encryptions the same, though? I would hope that when I purchased something from the National Geographic store in Washington DC, using my credit card number, that that number is encrypted in some form or another. Is that the same as somebody laundering tens of millions of dollars out the door of Australia in drug proceeds?

Mr Irwin—We would not be interested in finding out your credit card number, but we would be interested in finding out about any conversations or arrangements that were made in the latter case.

Mr HARDGRAVE—In the encryption process do the codes and whatever has been encrypted all look the same? Is there a deeper encryption than not?

Mr Irwin—My understanding is that encryption is becoming stronger and stronger. I cannot talk in terms of any technical understanding of how it is done. It depends on various mathematical formulations. My understanding of it is that encryption can be made stronger and stronger and more and more difficult for law enforcement to intercept unless it has the keys to be able to do it, even to the extent now that, as I have seen demonstrated, text can be hidden in visual images and photographs and so forth that are transmitted over the Internet. Again, I do not know if Mr Whiddett has any greater knowledge or experience in that area, or perhaps more technical expertise.

Mr Whiddett—Probably not technically. It is true to say that the sophistication of encryption is increasing apace, but the real issue for law enforcement is time. If you have something encrypted, there is the possibility that if you spent long enough at it you may be able to de-encrypt, but the difficulty for our line of business is that a lot of things are occurring in real time or, in prospect, occurring within reasonable time. Therefore, even if you were to bring to bear the most powerful computers, you would get no particular satisfaction in being able to crack it, say, weeks or months or years down the track. It is really a question for us of saying, 'Does encryption give someone an edge which is fatal in an investigation which is on foot?' The answer is a resounding yes.

Mr HARDGRAVE—It would be simpler for a bad guy to use a usual banking service, set up a bogus company anywhere on the Net and use that as a way of running whatever business he wants to run, than to try and set up some elaborate underground banking system using smart cards to deposit money onto it to take it offshore. It would be easy just to use existing legitimate circumstances.

Mr Whiddett—Depending on what the transaction is, at some point a commodity or money has to be somewhere to be converted into something that goes somewhere else. There is that, but there is always the question, of course, that you can have an exchange between two groups which is more to do with an accommodation, a promise to do something perhaps, on the understanding of some remittance. That is one aspect of it, too, or just sending communications about something.

Mr HARDGRAVE—Are we likely to see or have we started to see, on the basis of the way technology is going, cyber-havens, as we have tax havens and gambling havens? Are we seeing any evidence of that being set up?

Mr Irwin—I think there have been a couple of so-called kingdoms that have been set up in various parts of the world. I cannot remember what the names of them are, but there are at least a couple where people have tried to set them up as countries and have been trying to attract investment through various scam schemes. My understanding is that one of those has recently been closed down, but another one still currently exists and is the subject of as many warnings as people can give. They are the only ones I know of at the present time.

CHAIR—Can we be clear on this encryption issue. What are you advocating? Are you saying that, if there are encryption devices which would be difficult to break, they should not be

readily made available to the public, or are you saying that they should only be sold under government licence to approved purchasers? I am trying to be clear about what it is that you think we should do, as a country, to deal with the obvious problem of encryption devices that fall into the wrong hands.

Mr Irwin—My own view on that is that trying to stop encryption is probably like King Canute trying to hold the tide back. Given that there will be encryption, and given that there are legitimate reasons for encryption for the example that Mr Hardgrave has given in relation to his credit card, what law enforcement needs is an ability, in appropriate circumstances, to be able to go behind the encryption. That may be something that has to be done by virtue of judicial warrant. It is suggested, as set out at paragraph 2.3 of the submission in relation to the English legislation, that that act enables companies to be required to install equipment that would allow authorities to intercept and decode email messages. It is something of that sort that law enforcement needs, rather than a complete bar on encryption, simply because I do not think that it is realistic to prevent encryption.

CHAIR—We are talking about new technology devices and the problems that they present to you. The courts have shown, it seems to me, over some time a willingness to accept technology in a number of ways—obviously, fingerprinting was one of the early ones, DNA evidence and radar guns; what that provides is all now accepted—but clearly there are problems in some areas of technology in prosecuting crime. I think the Tasmanian submission talks about the problems of digital cameras, because the picture you get off a digital camera can be interfered with on a computer relatively easily. Whilst I am aware that law enforcement officers are all fine souls—

Mr HARDGRAVE—But not so technically literate as to be able to do it, perhaps, Chair!

CHAIR—We will not go into that. Apart from the encryption devices, from your knowledge can you give us a feel for some of the evidentiary issues that arise when you go to the courts. What other still-emerging areas do we have problems with?

Mr Irwin—I am personally not aware of any particular areas at the present time. That is not to say that, further down the track, problems are not going to emerge. The courts seem to be willing to accept electronic communications as evidence in the same way as they have previously accepted documentary evidence, provided there is proper authentication of the material, and I am not aware of any cases to date where there has been any major problems. I can see, however, that some of the complications that might be involved in presenting the evidence and explaining to juries how particular evidence may have come into existence might be something that can be used by competent defence counsel as a red herring to divert the jury, by making it all seem too confusing and complicated for them. That itself could be a problem, but I am not aware at the present time of any particular evidential problems that have been created by the new technologies. I expect that courts will move progressively to a stage where they will expect, particularly in complex document intensive cases, the evidence to be produced in electronic form rather than in hard copy form. I think the Victorian Supreme Court has a court set up for that purpose at the present time and I am sure that there will be a greater move of courts into the technological era. However, at the present time I am not aware of anything. Are you aware of any particular problem?

Mr Whiddett—I think there is just that residual fear that perhaps electronic data can be manipulated more than perhaps something that is written in a conventional form. But it will come to pass.

Mr Irwin—As I say, I think that is the area where defence counsel will work; to suggest that something like that might have happened, because it is all too complicated. Of course, the issue with the digital cameras is a significant issue for everybody. It is not only law enforcement which, it might be alleged, has the capacity to alter the evidence by using that sort of digital technology. At the present time it would rely upon cross-examination and credibility to try and determine those issues.

CHAIR—I have recently acquired a digital camera and, thanks to the shortcomings of certain government computer equipment, we are having great difficulty in getting the picture off anyway.

Mr HARDGRAVE—I want to finish on the question of legitimate versus illegitimate transport methods in the electronic sense of transactions. By sheer volume, by the sheer fact that encryption is so commonplace, again you have to find some interface, some point where digital signals are turned into dollars or cash so that you can do whatever it is you want to do—or do you? One suspects that once you have a whole set of credits caught up somewhere you might be able to transact elsewhere. What I am driving at is, rather than a bad guy or a network of bad guys setting up their own network, there are so many established networks now, so many legitimate ways to hide transactions, and for good reasons, like my credit card, that really the technology is helping the bad guys and saving them money. They just use legitimate means. What you are saying is that at some stage or other there is going to have to be a law which allows you to say, 'Hang on a moment, that is X bad guy—lots of encrypted transactions drawing attention to him or herself. We're going to go and get behind that encryption and find out what's going on.' That is what you want, isn't it?

Mr Irwin—Hopefully in advance, so that you know that the transaction is going to take place. What we do now, of course, with telephone interception—and I do not think it is any secret to anybody—is that you are hopefully listening to the bad guys talking to each other as they are planning and plotting what might ultimately come about. So you have some advance knowledge and, therefore, you can put some plans in place to catch them in the act. You would be hoping the same thing would occur with encrypted transactions.

My observation would be that, if somebody is going to use, say, the banking sector to try to launder their money, there will be some evidence of it somewhere that law enforcement can use. The problem for law enforcement is going to be more in the area where people are able to do things like use digital cash which they can pass from one computer to another without the intervention of third parties. The money eventually ends up in some tax haven country where it is difficult to get the evidence in any event. One of the dangers for law enforcement is that we are moving towards systems where people will not necessarily have to go through intermediaries or third parties to move value out of the country.

Mr SCHULTZ—This leads to my question which is: how successful has the Proceeds of Crime Act been? How will the system that you are talking about now improve it with regard to the seizing of assets that people may have, such as property and/or bank accounts?

Mr Irwin—The authority's position on this is that the proceeds of crime regime at a Commonwealth level would be much more effective if the Australian Law Reform Commission recommendation was accepted and what we had was a civil forfeiture regime, where the onus was turned back on the person with the property to establish on the balance of probabilities that they came by the property by lawful means. That is probably putting it a little bit simplistically. That is the sort of regime which exists in New South Wales, for example, and it has been extraordinarily successful there, because you have an agency, the New South Wales Crime Commission, which effectively pays for itself and leaves a bit over which can be put back into law enforcement and various social objectives.

I do not have the figures in front of me, but I know that if you compare, in the course of the authority's Swordfish investigations, the extent of the forfeiture of property and assets under the New South Wales legislation as against the forfeiture of money and assets under the Commonwealth legislation, the difference is almost like the difference between night and day. There has been a significant amount more seized and gone into law enforcement and government coffers under the New South Wales legislation than has been the case with the Commonwealth legislation.

Mr SCHULTZ—Because of the onus of proof—

Mr Irwin—That is right. The authority's position is that if we were to move at a Commonwealth level—and I expect that that may well happen, hopefully in the not too distant future, without trying to be too pre-emptive about it—if we were to move to that sort of regime right around Australia, then we would be a lot more effective in taking assets off criminals.

Mr SCHULTZ—That is a distinct possibility? I gather from the comments that you have made that the amendment to the act appears to be in the pipeline?

Mr Irwin—I think there is reason to be confident about it, given the findings of the Australian Law Reform Commission. It is something that I know is under active consideration.

CHAIR—I think it is a question to be directed to the government rather than to Mr Irwin.

Mr SCHULTZ—Yes, no problem.

Mr Irwin—I do not want to be too pre-emptive, but I think there is reason to feel reasonably optimistic that something will happen in the not too distinct future.

Mr HARDGRAVE—The only other thing I suppose that is left standing on a matter of national consistency is the gun laws. It is not even 100 per cent consistent in every state, but that is really the only time there has ever been a quick response to these sorts of crises that come up from time to time. I suppose being a QC you are a non-emotive person so you would never want to create a crisis, but one would have thought there is a crisis there—criminals driving a truck through this turfdom approach that has continued on after 100 years of Federation. We need to address this as a matter of urgency.

Mr Irwin—I could not agree more. It is an urgent problem to be addressed. It is a significant inhibition—I will not say 'inhibition' on law enforcement; it is a significant advantage to the

criminals. Notwithstanding that, law enforcement, because it appreciates the problems and has plans to meet them, has been successful. But that is not to say there are not problems there and it would be so much easier to work without the different gauges, as you put it before.

CHAIR—The secretary reminds me that the Corporations Law is probably an area where the states, in fact, have given up their powers for the greater good. The point was made earlier by these witnesses that the drug problem in this country in particular is of huge and appalling dimensions. It is going to probably be the issue that focuses the country's attention on dealing with some of the matters that have been highlighted in this submission.

I thank you, Marshall Irwin and Adrien Whiddett, for coming this morning. We will probably invite you to come back some time down the track when we have talked to some of the other witnesses. As I mentioned earlier, we saw this as almost a scene-setting one. Your experience obviously is helpful to us before we go and talk to all sorts of other people who have made submissions. You have taken a couple of things on notice, so when you are ready if you could let the secretary have that, we would be most grateful. Thank you Hansard and thank you to the staff. That concludes this public inquiry hearing for today. I thank everyone for coming and I declare the hearing closed.

Committee adjourned at 11.43 a.m.