COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

Reference: Crime in the community

THURSDAY, 26 SEPTEMBER 2002

CANBERRA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

Thursday, 26 September 2002

Members: Mrs Bronwyn Bishop *(Chair)*, Mr Murphy *(Deputy Chair)*, Ms Julie Bishop, Mr Cadman, Mr Kerr, Mr Melham, Ms Panopoulos, Mr Sciacca, Mr Secker and Dr Washer

Members in attendance: Mr Cadman, Mr Kerr, Mr Melham, Mr Murphy, Ms Panopoulos, Mr Secker, Dr Washer

Terms of reference for the inquiry:

To inquire into and report on:

The extent and impact of crime and fear of crime within the Australian community and effective measures for the Commonwealth in countering and preventing crime. The Committee's inquiry shall consider but not be limited to:

a) the types of crimes committed against Australians

b) perpetrators of crime and motives

c) fear of crime in the community

d) the impact of being a victim of crime and fear of crime

e) strategies to support victims and reduce crime

f) apprehension rates

g) effectiveness of sentencing

h) community safety and policing

WITNESSES

Committee met at 9.03 a.m.

FORD, Mr Peter Malcolm, Acting General Manager, Criminal Justice and Security, Attorney-General's Department

MAIN, Mr Geoffrey William, Special Advisor, Proof of Identity Project, Strategic Law Enforcement Branch, Attorney-General's Department

MEANEY, Mr Christopher William, Assistant Secretary, Criminal Justice Division, Attorney-General's Department

MORRIS, Federal Agent Tim, Director, National Investigations, Australian Federal Police

ACTING CHAIR (Mr CADMAN)—Welcome to this private briefing. I have not been fully briefed on or prepared for this briefing. I take it that what the committee wants is an informal discussion and presentation process rather than an evidence giving process. Is that your expectation?

Mr MELHAM—I think the other point to be made is that there will be a transcript, and I take it that, unless there are objections to aspects of it, it may well be released in due course.

ACTING CHAIR—If there is confidential stuff that they want to tell us, then we should shut the discussion down. Federal Agent Morris, would you like to kick this off and give us a background briefing?

Federal Agent Morris—I would like to provide with you a brief overview of the Australian Federal Police perspective on identity fraud. Along with all other police agencies, the AFP recognises the enormous personal and societal impost that identity theft has on all Australians. We also see identity theft and, more broadly, identity fraud as being a fundamental part of many fraud offences. It is also a critical precursor of and facilitator for a range of other transnational crime activity. Identity fraud was highlighted as a priority issue in the Commonwealth, states and territories agreement on terrorism and multijurisdictional crime on 5 April. Later that month, the Australian police commissioners conference endorsed a continuation of the Australasian Centre for Policing Research's identity theft project. That project has evolved from a scoping study of the phenomena in Australasia to a program that will formulate the Australasian identity crime policing strategy. That strategy will concentrate on prevention, victim assistance, developing partnerships, education resources and legislation.

The Australian experience in relation to identity theft and identity fraud largely mirrors what we have seen in other countries. As such, similar crimes are committed against Australian citizens. The crimes may include the compromise or takeover of credit facilities through to the theft of mail or the illicit capture of electronic data from credit cards. We have seen that criminals can generate substantial profits from these activities and that the victims are usually individuals. But we have also seen that these victims suffer a loss of credit ratings and other compounding effects resulting from financial mismanagement.

A web site maintained by the California Office of Privacy Protection estimates that it costs about $US800 per victim to restore and resolve the problems that occur as a result of identity

theft, and that the residual effects linger from two to four years after the offence is first detected. Whilst individuals are often the victims of identity theft, I do not think we can limit it to them: there is also the government, and more complex frauds are also perpetrated on large businesses and corporations.

It is not uncommon for criminals to obtain identities from legitimate government issuing agencies. The problem is, we see, one of the proliferation of legitimate identification documents and the stand-alone nature of how the identity of applicants is verified by those issuing agencies. Once one compromised document is obtained the system begins to crumble, with the compromised document being used to substantiate an identity to obtain further proof and so on. So there are substantial gaps in the system; not through a lack of due diligence but, we think, through the sheer volume of identities issued by agencies. Adam Graycar of the Australian Institute of Criminology recently presented a paper stating that in 2001 the following means of individual identification were issued by the Commonwealth government alone: the Australian Electoral Commission handled 2.46 million applications and amendment forms; the Australian Taxation Office issued 500,000 tax file numbers; Centrelink processed 4.4 million new claims or resubmittals of claims; the Department of Foreign Affairs and Trade issued 1.4 million passports; and the Health Insurance Commission issued 3.97 million new or updated Medicare cards.

Of course, no system is impenetrable to crime. We are not necessarily advocating that a more centralised system take place at this stage. Based on the above figures, no system could prevent some compromise. If a centralised system were compromised, the impact could be substantial. The Commonwealth government has used data-matching activities to detect overpayments and benefits successfully in the past. We think these programs have been successful because they highlight the conflict in data submitted to various state and federal government agencies. While those activities have been directed at the recipients of government payments in the main, and controlled under the auspices of the data-matching assistance and tax act, they have highlighted some vulnerabilities associated with the fragmentation of the information held by various government departments.

The problems are also compounded when we start to take into account the use of documents issued by foreign jurisdictions and institutions and their use in identifying a person for Australian purposes. While DIMIA have put in place robust measures to protect Australia's borders from the use of false travel documents—taking into account there the compliance officers and the compliance officer network—the private sector may not be so well protected: for instance, the presentation to and authentication of a foreign passport by financial services industry employees in support of certain financial transactions. When we turn our minds to identities, we need to think in even broader terms—so-called 'outside the box'—and go further than just names and data formally submitted to government agencies. There are many other unique identifiers associated with individuals. These could include email accounts, telephone numbers and PINs. They are really only limited by one's imagination. A good example of one of these unique identifiers is SIM cards in mobile telephones. The AFP regularly encounters criminals in possession of numerous SIM cards that are rotated through various handsets at any given time, subsequently hampering the effectiveness of any lawfully intercepted telecommunications. Many of these unique identifiers may also have a primary use in terms other than for identifying individuals. These may include market research and commercial opportunities, and yet they can sometimes take on the status of a de facto identifier.

Advances in information and communications technology and the proliferation of such technology will make it increasingly likely that a victim will have no physical proximity to the offender and the opportunities for such actions will present more often. Equally, people are now able to access so many services via electronic means that their physical identity—including their biometric details: their DNA, their fingerprints and those traditional sources of identification that law enforcement agencies have used—is decreasingly relevant. It is now possible to develop a persona totally online and to interact with a whole range of government and commercial services using that persona. This offers greater conveniences for legitimate activities but also, unfortunately, for illegitimate activities.

In the criminal environment policed by the AFP, the real utility of identity theft and identity fraud for criminals lies in the suppression of the offender's true identity. We see criminals utilising false identities on a regular basis across a full range of transnational crime activities, including people-smuggling, drug trafficking and money laundering. Law enforcement inquiries and databases traditionally focus on individuals. If the individual can conceal their true identity they have a greater chance of success in their criminal venture: they have a greater chance of evading the various trip-wires we can put in place throughout society, whether that is at the borders or whether it is in relation to other activities that we engage in. Of course, the concept of identity comes to the fore in the high-tech crime investigations conducted by the AFP, where we see criminals stealing the identities of legitimate users of the Internet, gaining access to their personal data and acting with almost total anonymity. The actions of the criminals in this regard serve to undermine public confidence in e-commerce, and the effect on the psyche of the individuals is no less than if a person physically entered their residence and rifled through their personal documents. In one ongoing AFP high-tech crime investigation, the person of interest obtains and sells identities such as people's usernames and logins to others online. This person also provides a range of other services that would be particularly useful to criminals creating a new identity, including access to services provided by financial institutions.

As I said previously, it is the broad utility of the stolen or fraudulent identity that has the greatest impact on crimes policed by the AFP. The US government, as well as several US states, has taken a course of criminalising the act of identity theft. In October 1998, Congress passed the Identity Theft and Assumption Deterrence Act 1998 to address the problem of identity theft. Specifically, the act amended the law to make it a federal crime where anyone knowingly transfers or uses without lawful authority a means of identification of another person with intent to commit, aid or abet any unlawful activity that constitutes a violation of a federal law or that constitutes a felony under applicable state or local laws. Violations of the act are investigated by federal investigative agencies such as the FBI, the Secret Service and the US Postal Inspection Service. In addition, there are a plethora of US federal and state government web sites aimed at educating the public in relation to identity theft and providing an avenue for complaint to commence the resolution of any injustice.

Australia has taken a slightly lower legislative profile to date, and there are fewer web sites offering education and services to victims and potential victims. Part of the actions of the Conference of Commissioners of Police of Australasia and the South-West Pacific in this regard was to refer this issue of possible legislative changes to the Police Commissioners Advisory Group for consideration. The lack of specific legislation does not mean there is a lack of policy/legislative effort in the Commonwealth and the states. The recent studies by the

Attorney-General's Department and those coordinated by AUSTRAC are assisting in more accurately defining the scope and nature of this issue.

There have been several pieces of legislation designed to ensure a person is who they claim to be. For example, the 100-point identification test required by financial institutions for opening accounts stems from the provision of the Financial Transactions Report Act 1998. In yet another example, section 10 of the Passports Act criminalises false statements made by people in relation to obtaining an Australian passport. Offenders are liable for a $5,000 fine and up to two years imprisonment. The social security and tax acts have similar provisions. Indeed, one does not need to identify oneself when purchasing a mobile telephone service, due to provisions of the Telecommunications Service Provider Identity Checks for Prepaid Mobile Public Telephone Communications Services Determination of 2000. The AFP will be a keen participant in the Police Commissioners Advisory Group legislative study on this issue.

ACTING CHAIR—Excellent. Do Attorney-General's have any comments?

Mr Ford—There are a few comments I could add, Mr Acting Chair, if you wish—fairly briefly.

ACTING CHAIR—Yes, please.

Mr Ford—Identity fraud is presenting a growing threat throughout the world as false identities are utilised in a greater range of criminal activity. Also of concern throughout the world is identity theft, which has significant emotional and financial costs for individuals. Identity theft is a gross invasion of privacy and its prevention would increase public confidence in the security of their personal information. False identities are readily created by targeting weaknesses in the existing personal identification and authentication processes used by organisations.

The use of false identities may be a factor in terrorism, border protection, fraud, money laundering and electronic commerce. As a result, there is substantial and growing concern about identity misuse in many public and private organisations. Any significant advance in improving identification systems would need to recognise the critical importance of both birth and death registration records kept and maintained by agencies under state and territory jurisdictions and DIMIA people movement records. The negotiation of a partnership between the Commonwealth and the state and territory governments enabling each to have access to key registration data for the purpose of confirming identity documents would be necessary.

Work to address identity fraud is being undertaken in many agencies in the Commonwealth. The Attorney-General's Department has been given a lead role by the Heads of Commonwealth operational Law Enforcement Agencies to ensure a strategic direction for improved personal identification and authentication practices. To gain an insight into the extent and nature of the problem, the Attorney-General's Department undertook a study on the management of identity fraud risks within several Commonwealth agencies and produced a report entitled *Who goes there?* This report contains sensitive information about the controls operating in several agencies and consequently has a protected classification. Also of possible interest to the committee is an article in *Security Oz*, which I could table if you wish. As a relative newcomer to this area, I found it interesting to read.

ACTING CHAIR—Certainly; thank you.

Mr Ford—Effective solutions to combat identity fraud would require a coordinated whole of government approach. It would be possible to develop these solutions without adopting measures that are inherently privacy invasive. This would require consideration of limitations and safeguards as appropriate to balance the interests of individuals as embodied in privacy legislation with the broader public interests of the particular measure under consideration.

Finally, the cost of identity fraud in Australia has been roughly estimated to be $4 billion. The AUSTRAC committee, containing representatives from Commonwealth and state government agencies as well as representatives from the banking industry, is working on ways to more accurately assess the cost of identity fraud to the community.

ACTING CHAIR—Thank you. Are there any questions?

Mr MELHAM—There is something, and it is the complete opposite of what you are saying. I am staggered by the statistics, and I appreciate the evidence that you have given. At the same time, I want to also work out how we can help what I might call the innocent victims of identity fraud. Again, we all have personal experiences. I can recall my sister-in-law, having lost her bag. Her identity was assumed by someone else who was picked up for shoplifting. No fingerprints were taken per se, but that name then went into the criminal register and all sorts of hassles occurred in relation to her and verifying that it was not her. She had to go through a whole range of things. I am wondering if, in terms of this, we need to have that perspective as well, because they still become victims: the people whose identity has been taken from them then get caught up in the whole red tape situation.

I am just wondering what the different regimes are, and whether we need a uniform approach nationally, so that, in effect, when people establish: 'It wasn't me; it was an assumed identity,' they themselves do not become ongoing victims of that identity fraud when they go to the bank, when they go to do something else or if they are, for instance, picked up in a random breath test or whatever and that name comes up as someone who is also known through an alias as a murderer, rapist, armed robber or whatever and all the red lights light up. Are you able to tell us what protections are in the system? Have there been improvements in where we are heading in relation to that? Do you understand that I am talking about another class of victims—not just the community but innocent people whose identities have been tainted?

Mr Ford—I will ask Mr Main to answer from the department's point of view.

Mr Main—There is some pilot work being undertaken by the Australian Bureau of Criminal Intelligence to build a database of lost and stolen documents and false identities. The agencies involved in the pilot are some Commonwealth agencies, some state departments, some law enforcement agencies and the banking community. The pilot has only been running for nine months at this stage, but I understand from a briefing I went to a few weeks ago that things are going very well. The idea of the identity fraud and document theft register is to allow those government agencies that are processing new claims for individuals to do a check online against the documents that they are being passed to see if they have been listed as lost or stolen. I think that is only a part answer to your question.

Mr MELHAM—It is an answer that goes a long way to resolving the issues that I have raised.

Dr WASHER—It is staggering: $4 billion dollars a year is a lot of money.

Mr SECKER—Four hundred bucks for every man and woman.

Dr WASHER—It is a heck of a lot of money. E-commerce is the issue I would like to pick on, because it is the one I know least about. There seems to be apprehension about what you can actually do to secure that. Firstly, should we be educating our public better about the precautions they should take in using e-commerce? I have not seen much education stuff for general public consumption. Secondly, what are the safeguards in this? What are the real risks in e-commerce? Is it safe to use e-commerce in this country? Is the legislation we have got adequate to punish people accordingly for crimes committed?

Federal Agent Morris—I will answer in part. There was a new suite of computer crime offences introduced in December 2001 which gives Commonwealth law enforcement agencies a fair degree of scope in prosecuting and investigating the types of people who enter without permission other people's computer systems and alter, change and steal data. That has converged with an increased capacity in training—across the Australian Federal Police, at least—with the skills of the officers, the legislation and the technical ability to actually investigate these crimes effectively. So we have certainly made progress in the ability of law enforcement to take action—unfortunately, once the crime has been identified and reported. Certainly education and prevention are going to form a major plank of the Australasian police commissioners conference strategy in terms of identity fraud. I think that is an area we can do more work on, in terms of educating the public in future.

I am not an electronic commerce expert. Obviously people have varying degrees of confidence in using electronic commerce. Some people are very confident and do most of their financial institution transactions online, whereas other people are still very reticent to divulge, for example, their credit card numbers for an Internet transaction. So it is gaining acceptance but there will always be some suspicion, particularly by older users who are not so confident of using the technology.

ACTING CHAIR—Excuse me, I have to go to the chamber. Mr Murphy will take the chair at this point. I have to go down to the chamber for a short while to make sure that enough people are there to start the parliament, but I will be back.

Mr MELHAM—He needs to pray; there is a lot to pray for.

ACTING CHAIR (Mr Murphy)—Mr Meaney, do you have anything to add to that answer?

Mr Meaney—Yes, Mr Acting Chair. One of the fundamental problems is that there is an inherent tension between providing a secure system for e-commerce and something that is commercially friendly. Clearly, it is going to be in the interests of business to have as few hurdles as possible so that commerce can be facilitated. We have all probably had the experience where you can ring up over the phone or the Internet and the only identification that you need is the credit card number. You read out details of the number, the expiry date and the

name on the credit card, and that is about all that the person on the other end ever actually knows about you. Whilst it would be desirable to have a far greater integrity about that process, of course there is a bit of a conundrum here: every time you put some sort of integrity into the system there can be resistance because it can make the process less facilitative. So there are always balances about how far we can actually go, I guess.

Mr Ford—I will just add another point to that. I recently chaired an exercise within the OECD to develop security guidelines for information networks. It is a much broader topic but it does touch on this, because it was recognised by all the member countries that there does need to be a component of education in that. The basic idea was that, just as we are all used to looking both ways when we cross the road, locking our cars and those sorts of things, users need to become more savvy in terms of using. That requires an education program of some kind.

Dr WASHER—But that seems sadly lacking. Certainly I do not know. Patrick, do you know all the security issues? I am sure Daryl does not know. There would be three people here who would not know. Have we been pushed into e-commerce? To do work with the ATO, you have to do it by electronic transactions. Banks encourage it, otherwise the costs start to escalate. In other words, they punish you via punitive measures of cost if you do not do electronic transactions. I guess it is about education. It is about prevention as well, which we do not really have. Us guys do not have the remotest idea what security we should be using. I certainly do not, and I guess a lot of other people out there do not either. It is a high priority, because it is going to mushroom. That is a hell of a loss: $4 billion. And it is not just that, but what is to come.

Mr SECKER—I think we have got to look at two areas. Firstly, do we have the resources to prevent this sort of crime and, secondly, if we cannot prevent it, can we catch the criminals? Are we spending enough money? Are we setting up the investigative networks that you need with the expertise in computer crime to actually catch the fraudsters?

Federal Agent Morris—From an AFP perspective, I think we are increasing in a fairly comfortable relationship with the way the use of e-commerce is expanding. The investigations that we are taking on tend to reflect that. We are trying to do the high-end ones. Bear in mind that a lot of these simple frauds do fall under state jurisdictions and clearly are in the ambit of the state and territory police to address.

Mr SECKER—Are they working together? It would seem to me that if we are going to have an international network—there is a possibility—of things on e-commerce the states should be getting together, at least on a regular basis, to say, 'Well, we're doing this. We found this,' and so on.

Federal Agent Morris—I think the clearest expression of that is the identity crimes scoping paper, which is the forerunner to the identity crimes strategy that the Australasian police commissioners are putting together now. I think the benefit of that will be a consistently implemented strategy across the state and territory police and the Australian Federal Police across Australia. So if there is not undue emphasis in some areas, it is certainly going to be raised by the endorsement of the strategy by the commissioners and then the subsequent reporting back on the implementation.

Mr Meaney—I guess that also raises the question—this point is very much addressed in the paper that Geoff might speak on a little later, and which has, I think, been distributed to you all—of the fundamental integrity of the things we use as identifiers in society. In general, you go to your video shop or whatever. If you need an identifier, people will accept your drivers licence. The question then is: can you guarantee the integrity of a drivers licence? They are usually based on other documents: for example, birth certificates. Then we get back to whether you can guarantee the integrity of birth certificates. Ever since the infamous book *The Day of the Jackal*, everybody knows you can go out and get a false passport, because there is a nice little guide encapsulated in the book which shows you exactly how you do it.

Mr MELHAM—Irrespective of the guide, there are people who will do anything for money, aren't there?

Mr Meaney—Exactly. But it is far easier to exploit systems that are not integrated and have a fairly low integrity rating than it is something that might have a higher threshold or a higher integrity associated with it. That then leads you to the debate that will inevitably ensue about whether you should have something like a national identifier, and clearly, there are civil liberties concerns about the issues surrounding national identifiers. Geoff might speak a little bit more about some of those issues. National identifiers are, of course, very common in relation to civil code jurisdictions. They have not been traditionally part of the common law system, but certainly in civil code European countries the idea that you need to carry some sort of identification which is a national identification system is not uncommon.

Again, Geoff might be able to give you a little more detail, but I understand that the UK, for example, as part of the pressure that has come from the EU, is looking at a national identifier that is in some ways similar to the national identification processes used by most European countries. These are sort of the core issues. If you are going to go to the point of trying to have a high integrity identifier for individuals, there are going to be people who see this as an infringement on their civil liberties. Inevitably, striking the right balance is the big issue. I will ask Geoff to talk a little about some of the developments overseas in relation to identifiers. He has some interesting information about one of the ones that is pretty well known—the US social security number.

Mr SECKER—That has been around forever.

Mr Meaney—Even that has problems, as I understand it.

Mr Main—I might just pick up on some of the preventive aspects that your question alluded to. There is quite a lot that we can do to strengthen the existing front door processes that organisations have when they check the identity of an individual. It has been mentioned this morning already, and you would be aware, that those processes are quite deficient. They are legacies of the past when the threats to false identity were not as high as they are now. So organisations basically accept a wide range of documents that come from a whole lot of organisations. A lot of those documents—in fact, most of them—have very low integrity. The problem with that is that those documents of a low integrity that are easy to obtain or are easy to forge or manufacture can then be used to get a document that is a little bit more important and of a little bit more value to the individual, thereby enabling them to move up to a document that can be quite sound and that will be accepted in most places.

Those processes could be improved if we were to standardise the documents that were accepted and we took only a few of those documents that were deemed to be of higher integrity. We need some sort of process that sits behind that front counter work to allow the customer service officer to be able to check that the document they are being given is in fact a document registered with the issuing agency. Those sorts of confirmation processes, if we might call them that, basically do not exist in our community.

There are some things that some organisations will do for particular applications that raise warning bells and that they will check with the organisation. But they are very timely processes. You would be aware with the huge number of registrations being done in Australia each year—we heard some figures earlier about organisations typically doing hundreds of thousands, if not millions, of new registrations or changes each year—there is a huge time issue in checking each document that comes through. We need to be able to provide those officers doing the checks with maybe some sort of online real-time facility to be able to check those documents of greater integrity to make sure that they at least have been issued by the issuing agency.

Mr Meaney—I guess this is also important to the point Daryl Melham made earlier, which is that if you do have a register of lost and stolen documents, for example, a simple check could be whether or not the document being presented to you has been reported as being stolen or something like that. There are those sorts of checks.

Mr MELHAM—I recognise that with technology and the advances that have made that criminals are going to find new ways to defraud. When something is no longer working and you close that loophole, they will find another loophole. It is like the honest businessmen who look at our tax act and other laws; they are not dry and they have found a loophole. I am interested from a government point of view in whether there is an economy of scale as to how far you can actually go. We cannot kid ourselves; this stuff is going to continue to happen where there is money and drugs and that sort of stuff.

Mr Meaney—You are never actually going to stamp it out. All you are really doing is raising the hurdle.

Mr MELHAM—It is about having cross-checks or whatever. As I said, when you talk about passports or whatever, if you have a corrupt official, then you can get a good document. But it is a question of them being able to have security checks to catch the corrupt official.

Mr Ford—The argument really is about reducing the impact of it and reducing the cost.

Mr MELHAM—Absolutely. I think we need to be honest about that. I am concerned about the false impression out there that we can actually stamp this stuff out. What we are trying to do is minimise it and give ourselves the best chance of exposing it. It is like zero tolerance in terms of drug strategies. It is garbage. It is just not achievable, and it does not do the fight against drugs any good to have that public perception. I do not need to go into it, but I make it as a statement of fact.

Mr SECKER—We probably have zero tolerance for fraud.

Mr MELHAM—We want zero fraud. We want zero drugs and all that. There is no problem with that. But the perception that anything we can do can stamp it out completely is crazy.

Mr SECKER—I do not think there is any argument about that.

Mr MELHAM—It is like putting your finger in the dyke and then working out where you can be most effective. You are fighting on a number of fronts. I am interested in whether there is this an ongoing strategy of monitoring and what is the lifespan of the systems that you are putting into place. I know it is like computers and software: it will last you two or three years and then you have to get a new computer because they have new gadgets on them. Is it the same here in terms of the technology?

Dr WASHER—Most of them stop working after about thee years anyway, Daryl.

Mr MELHAM—It is just that you did not have to worry. When I walked across Spain recently on the Camino, I did not have to worry about computer fraud or e-commerce fraud because their life is much simpler. They did not have these things in their life.

Federal Agent Morris—I think also there is a continuing spectre that we are a multicultural society. We are part of the global village. There are going to be people with all their documents issued by foreign jurisdictions living, residing and working in Australia. It is terribly difficult to validate the authenticity of a lot of those documents. No matter how good the systems we put in place are domestically, it is a fact of life that there will be people with foreign passports and identity documents wanting to do business in Australia.

Mr MELHAM—My understanding—correct me if I am wrong—is that if it is coming from a particular country, you would have a register. It is like the Department of Immigration and Multicultural Affairs. If you have education qualifications or whatever, they will go and get certain ratings. I take it you have that system in place and that you do not just accept them on their face.

Federal Agent Morris—No. That is DIMIA.

Mr MELHAM—In other words, it is like a high alert. If you are dealing with this particular document, it is something you are not going to accept on the face of it.

Federal Agent Morris—Absolutely, but I think that has to translate into the private sector as well.

Mr MELHAM—That was my next question.

Mr Main—I wonder whether I might build on that discussion. One of the useful things we might be able to do is to look at the births, deaths, marriages and change of name data and pool that with the movements data. The state Births, Deaths and Marriages that hold that data. If we were to pool that with the immigration data, the movements data, arrivals, departures and citizenship, we would have an idea of who is in the country at any one time. We would not know, with the example of someone coming from overseas, whether the travel documents they had were legitimate or not, but we would know that they were going to use that name once. If

we could get an idea of the net population and subtract from that deaths and departures, and then we added to it new births and arrivals, that might at least give us a fundamental idea of who should be here. Then there are other issues to do with maybe checking life events to make sure that people have been around and they have been doing actions in society to show that they have lived for a long enough period in the society. But I think the first part of that suggestion might have merit.

Mr MELHAM—Thank you.

Dr WASHER—I want to build on that while we have Mr Melham here, because I know how Daryl feels about the loss of liberty. I think Daryl would hold probably a very strong position on individual liberties. But surely the mood is changing now throughout the world, particularly in countries like Australia. If you do not have good identification techniques, loss of life is also a real risk. It is a really serious problem these days in terms of security. So that liberty factor I do not think is quite as strong as the intimidation factor. We can have people moving through our society as terrorists, as criminals or whatever in some illegal way and we cannot identify them because our technology is compromised and because we have not gone through the process of establishing accurate identification methods and making people identify themselves accurately. I think that mood has shifted—is that your feeling?—compared with a couple of years ago.

Mr Main—My feeling, from speaking with a number of Commonwealth government agencies who prepared the report you have in front of you, is that that is definitely the case.

Dr WASHER—Daryl, I am interested in your comments. I understand where you are coming from. You champion liberties to the ultimate if you can, but don't you feel it is a balance that is starting to swing against individual liberty and that, in terms of a lack of accurate identification, the mood is changing?

Mr MELHAM—In what way do you say it is changing?

Dr WASHER—Once upon a time they said everyone had to carry the Australia card. That was a few years ago. You had to carry a card of identification on you all the time to go anywhere or do anything.

Mr MELHAM—That is one of the things I opposed.

Dr WASHER—know.

Mr MELHAM—I still do.

Dr WASHER—That is why I am asking.

Mr MELHAM—I oppose it is for this very reason. If this is the identifier, do not think that criminals cannot get themselves an Australia card and give themselves access to a whole range of things. This notion that an Australia card will fix our problems is just garbage. Criminals will be able to get themselves an Australia card and then they too can run rampant. These are my thoughts, Mr Main. If you want to come in on this, please feel free.

Mr Main—I would just like to add that that has certainly been the experience all around the world when they have brought in these single common identifiers. Basically, these things have been built on moving sand, foundations of sand, and they are only as good as the data that goes into building them. If the data that is going in to build them is garbage then, yes, I agree. Can I just speak theoretically?

Mr MELHAM—Sure.

Mr Main—It would not work unless it was possible to build an unassailable register of all residents and citizens in Australia and maintain that register so it was unassailable.

Mr SECKER—So it would also include those visiting from overseas and those Australians who are overseas?

Mr MELHAM—The only way you could probably make it unassailable would be if you basically had something whereby you could look into a computer and it could register the eyes, the fingerprints or whatever. What is shown in the sci-fi shows we have seen is the only way you are going to get something that cannot be used and abused, because you then know it is that person.

Mr Main—That is right.

Mr Meaney—Even that, just to be devil's advocate, can be abused, because whilst the biometrics—the actual scan of your eyes or your DNA or whatever—can be accurately logged, it is only as good as the computer in which it is stored. Clearly data can be manipulated in a database.

Mr SECKER—And who puts it in.

Dr WASHER—They could go along and say, 'These are my eyes but my name is Mal Washer.'

Mr MELHAM—So what I am saying, Mal, is that you would probably get away with it. Whilst on the surface it looks as though it could solve the problem, you actually create other problems because of the inventiveness of criminals.

Mr Meaney—You get a false sense of security because you think this is an unassailable thing.

Dr WASHER—I was going to build on this, Daryl. I knew the Australia card would bring you out, and I am glad to hear that. I got Daryl out. He has woken up and it is good. I knew he would say that. He is saying—I think it is what he is saying—that people do not want to compromise liberty and be inconvenienced unless we have something that makes it worthwhile.

Mr MELHAM—Exactly.

Dr WASHER—So, hypothetically, apart from having everyone documented on some database that you have to access, what could we actually give people? What do you imagine we should have that someone should carry and that would be an accurate identifier? What can we do? Is there anything we can ever do? Apart from major surgical implants or something—that is, going with something crazy—is there anything we can do?

Mr Meaney—Before he gets to answer that, I do not know whether you have seen the latest Tom Cruise movie, but they use the eye scans as the basis for it and then they transplant his eyes. You can even get around that, by the look of it. That is science fiction.

Dr WASHER—You could take out the other guy's eyes and stick them in front of the lens.

Mr Meaney—He walked into the shop and they said—

Mr MELHAM—The eyes have it.

Mr Main—I think we can prevent a lot of the false registrations through having processes in place at the front door to make sure that those people registering for goods or services have been born or have arrived in Australia and are not dead. Those sorts of things could be the fundamental things we build on. We would probably also want, at the same time, to complement those preventive processes by cleaning up our existing registers. I know there is a lot of work being done.

Mr MELHAM—There should be cross-checks and audit trails.

Mr Main—Yes, and very well-defined ones, working closely with the Privacy Commissioner's people to make sure that there are well-defined data matching exercises to clean up those existing Centrelink registers, Australian Taxation Office registers and the sort of things where we do know that there are spurious and redundant records. Some of them are fraudulent. For whatever reason, they are there and they do cause problems. The 'Numbers on the Run' inquiry, as you would be aware, found that between three million and four million—I do not have the figure exactly—excess TFNs have been allocated.

Mr CADMAN—The public are generally unaware how secure the services are that they are using for electronic transactions in particular. Has anybody thought about how it might be possible to grade the security factor in some of these, be it banks or building societies, right down to buying stuff online and all that sort of thing? It seems to me that the prospect of stealing an identity through electronic processes is becoming quite easy. I think as you said in your opening remarks that you only want one weak factor, you only want a starting point, and then you can build on it and get a drivers licence or whatever.

Federal Agent Morris—Some of the financial institutions have floated the idea of being able to validate documents online with the issuing authorities. That would be their perfect world. So if someone hypothetically comes in with a birth certificate saying that they are Mr Tim Morris, they will be able to validate that online with Births, Deaths and Marriages and know that that birth certificate is actually good, that no subsequent death certificate has been issued and so on. Some elements of private enterprise have an idea of where they would like to go in terms of

very practical alternatives to ensuring that they know who they are dealing with. I would certainly raise that as a possibility.

Dr WASHER—At the moment, would you folks sitting over there be happy to purchase things online from overseas, like the US, through the Internet system?

Mr Ford—I have done it.

Dr WASHER—And you feel secure about that?

Mr Ford—I think it is a matter of balancing the risk. All I have bought is books, but they have turned up.

Dr WASHER—I guess the question then is whether it is hard for other people to access and use that information you transmitted.

Mr Ford—There is a risk.

Federal Agent Morris—As I understand it, there is very little interception of people's private details as they are being transmitted from one location to another. The bulk of crimes where people's personal identification details have been stolen—credit card numbers and identifying factors—has actually been from a deliberate break into a company's network, where someone is looking for these details and removes them.

Mr Ford—It is like using your credit card anywhere. If there is a dishonest employee on the other side of the counter, they might use it.

Mr CADMAN—Somebody breaking into that company looking for credit card details physically?

Federal Agent Morris—No, online.

Mr CADMAN—They are breaking in online; getting into the computer?

Mr Main—They are hacking in.

Mr Ford—Sorry, I should have clarified that.

Mr CADMAN—Are all transactions, whether they are physically across the counter or online, stored electronically anyway?

Mr SECKER—Some countries are more secure than others. You would not in your right mind even use a credit card in Nigeria, for example. You just do not use one.

Mr Meaney—You certainly do not give them your bank account number.

Federal Agent Morris—In Malaysia they do not accept Visa card up there anymore. There are big signs saying that they will not accept Visa because it has been compromised so widely. Certainly criminality has had an impact in some jurisdictions to the point where it is no longer commercially viable to run some of those uses.

Mr CADMAN—You reckon the cost to an Aussie would be about $800?

Federal Agent Morris—Approximately $US800 was the figure, and I think it is 175 hours in a person's time trying to retrieve and clear up the damage caused by the theft of their identity.

Mr Meaney—This is, for example, if you get something on your credit card bill. This happened to me some time ago. There was a transaction in the United States when I was not in the United States and had not been to the United States. It was clearly fraudulent. I think the cost that has been talked about here is about the time and effort it takes you just to retrieve that through the normal credit card processes, to get it taken off, the number of times you have to approach them to get it fixed up and to get interest for that transaction taken off. This is just the cost to the individual of rectifying it. Even if it can be readily established that it was fraudulent, there is still that cost to it, let alone if it is more significant.

Federal Agent Morris—You would have to go back to credit rating agencies and restore your credit reputation. It is quite time consuming.

Mr CADMAN—I notice that this random survey says it was to be published in 2001. Has the random survey been done?

Mr Main—No. It was a suggestion we proposed that some of the other Commonwealth agencies might like to join in doing that work. The idea was to get 1,000 or so representative customers from the databases of those main agencies and to check them out to the nth degree and thereby get some idea of the incidence of falsities.

Mr CADMAN—You use the words, 'this will provide an improved'. Perhaps it should be 'would'.

Mr Main—I think when I wrote that I was probably hoping that something would come off. It did not get a guernsey. What is happening, though, is that through the AUSTRAC Proof of Identity Steering Committee that a number of Commonwealth, state and law enforcement agencies and banks are on, there has been some money put aside to get a contractor in SIRCA, the Securities Industry Research Centre of Asia-Pacific, to do a cost of identity fraud survey. They will be using a different methodology because they will not have the access that I was hoping to get to those individual customer records. They will be doing it using aggregate statistics and trying to come up with some methodology that allows them to predict what the undetected rate of fraud is, which is a critical thing in all of this, of course. It is quite easy to go and ask organisations how much fraud they find and add it up. But there is another component to it and that is the undetected amount, which is critical, as well as all those other non-financial costs of course.

Mr CADMAN—I take it, because it is your first recommendation, that you have consulted widely, and everybody here would regard that as one of the most significant things that could be

done. If that is not the case, it is one of a number of things. Could you let us know, because that could well form one of our recommendations, I suspect.

Mr Main—A couple of the agencies, such as the tax office and HIC, had some privacy problems with making the data available for the sorts of checks we want to do.

Mr Meaney—Perhaps we could do a subsequent paper to the committee on what actions have transpired.

Mr CADMAN—It seems to me that the tax office ought to do their own integrity check. Provided you laid down the criteria, they could do it themselves and other agencies could do the same. Then, having verified—perhaps not disclosing to each other—whether there were duds in the system, there could be a data matching process between them on either the same names or a random sample. You would get some results that way, wouldn't you?

Mr Main—You should do. It should give you a very good insight into what the whole problem of identity misuse is, because it is not all fraud. It is that whole spectrum of identity misuse, running from people using multiple names of convenience to identity theft. We would get a good idea of what the range and extent of it was.

ACTING CHAIR—Federal Agent Morris, do you think the AFP is getting on top of the importation of narcotics, particularly heroin?

Federal Agent Morris—The current statistics reflect that we have never been more successful than we have in the recent past. There are a whole lot of reasons that we might attribute to that success. There have been different international factors in terms of droughts in traditional opium growing areas. There is also the focus and the funding under the National Illicit Drug Strategy. The AFP has set up the mobile strike team specifically to look at serious drug trafficking and importation. The expansion of the overseas liaison network that provides us with intelligence and the greater leads to focus at the very highest levels of heroin importers has made a significant contribution in that regard.

ACTING CHAIR—What are your views about the heroin trials going on in Australia?

Federal Agent Morris—My personal views?

ACTING CHAIR—Yes, from your experience.

Federal Agent Morris—I have only recently—five months ago—arrived back from Singapore. I spent the previous three or four years over there. I have not had an opportunity first-hand to examine the effectiveness or otherwise of the heroin trials. I have watched with interest what has been occurring in Kings Cross in Sydney. I understand there is going to be an evaluation of that after the next state election, if I am not wrong.

Mr SECKER—They would not do it before, would they.

Federal Agent Morris—No. I very much have an open mind to see what comes from the results.

ACTING CHAIR—Do any other members of the committee have any other questions? We need to wind up shortly, unless there is anything pressing.

Dr WASHER—Can you see a future where we should do DNA tests on every individual in the country? At the moment, we do it for people suspected of serious crime or who have committed a crime. Could you see, apart from the problems of freedom, any advantage in it?

Mr Ford—I doubt it. Again, it is not something personally I have had any involvement in. I doubt that there would be scope for taking DNA from everyone. Just harking back to the discussion we had before about balancing privacy and law enforcement, you would need to be convinced—

Dr WASHER—And you would need to determine whether it was cost-effective.

Mr Ford—Exactly.

Mr SECKER—What would it cost to gather 20 million DNA samples from around Australia? You could staff a hell of a lot of hospitals for that.

Mr Ford—You would also need to be sure, even before you considered the balance, that it could not be circumvented easily. Otherwise you could be in a worse situation than when you started if you had something that was apparently inviolable and yet corruptible.

Mr Main—I think that is a good point. The DNA details would need to be stored on computer somewhere. There would be a series of zeroes and ones, I would gather. If that series of zeroes and ones could be picked up in the right order, then we could probably steal it and assume someone else's identity. That would be of concern.

Mr CADMAN—The first identifying factor is the critical one, isn't it? My brother, when he applied for his Medicare card, included his dog on his card because he was at the vet so much. So he put Sally Cadman on his card. Sally Cadman has been on my brother's card as eligible for Medicare for 10 years or more. She died and so he told them that they had better remove her as she was not living at home any more.

Mr KERR—Spotty Taylor was a dog who got elected to the administrative committee of the Labor Party once.

Mr SECKER—He probably did a good job too.

Mr KERR—It was never revealed, because it was designed to show the inadequacy of the then scrutiny.

Mr CADMAN—It succeeded.

Mr KERR—It never happened as such. The point was it would have happened but for the fact that the people who did this were saying, 'Look, see how easy it is to do.' There you are, a confession from the Hon. Alan Cadman. Both sides of politics share these whimsies.

Mr SECKER—On a cost-effectiveness basis, I would have thought there was going to be more success in a very tight area. Examples include what they are doing on Norfolk Island or in that town in Western Australia, where they say, 'It is not going to cost us so much and we might clear it up.' It is probably going to happen only after all the other areas have been exhausted and they have not got anywhere. But it would raise all sorts of other problems, like in paternity cases.

Mr Meaney—Yes. You could see thousands of marriages maybe going west.

Mr SECKER—Exactly.

Dr WASHER—The Child Support Agency has enough problems as it is.

Mr Meaney—We will get back to you with that submission that we foreshadowed of an update on what has transpired since the preparation of the report.

Mr CADMAN—Your submission this morning has been really helpful. We will get an update on this report and where it is moving to. From my perspective, they are good recommendations. It would be helpful to have an update on that.

ACTING CHAIR—On behalf of the committee, Mr Ford, Mr Meaney, Federal Agent Morris and Mr Main, I would like to thank you very much for your briefing this morning.

Committee adjourned at 10.03 a.m.