

LAW REFORM, DRUGS AND CRIME PREVENTION COMMITTEE
**Inquiry into the supply and use of methamphetamines, particularly ice,
in Victoria**

Canberra — 11 February 2014

Members

Mr B. Carroll
Mr T. McCurdy
Mr S. Ramsay

Mr J. Scheffer
Mr D. Southwick

Chair: Mr S. Ramsay
Deputy Chair: Mr J. Scheffer

Staff

Executive Officer: Ms S. Cook
Senior Legal Research Officer: Mr P. Johnston

Witnesses

Mr D. Smith, CEO, CrimTrac.

The CHAIR — I officially declare this public hearing open and welcome our witnesses this afternoon: Mr Doug Smith, chief executive officer of the CrimTrac agency, Ms Jane Diedricks, who is director of legal and Mr Andrew Paterson, chief of staff. Welcome to the three of you. We also have members from the Australian Institute of Criminology present — Mr Burman is here. We have Sandy Cook, executive officer, and Hansard at the back.

We are conducting an inquiry into the supply and use of methamphetamines in Victoria, particularly ice. We have as part of our reference particular reference to Indigenous communities and regional areas. We are probably about halfway through the inquiry in relation to gathering evidence. We have spent two days here in Canberra collecting evidence. I thank you for your time this afternoon.

Mr SMITH — Pleasure.

The CHAIR — I understand you are going to lead, but before you do I will read you the conditions under which you are providing evidence to this committee this afternoon.

The CHAIR — All evidence taken at this hearing is protected by parliamentary privilege in accordance with reciprocal provisions in defamation statutes in Australian jurisdictions as if you were giving evidence in Victoria and as provided by the Victorian Defamation Act 2005 section 27, the Constitution Act 1975 and the Parliamentary Committees Act 2003. Any comments you make outside the hearing may not be afforded such privilege. Any reporting of these proceedings enjoys qualified privilege for fair and accurate reporting as if the proceedings were in Victoria. Have you read the guide for presenting evidence to parliamentary committees?

Mr SMITH — Yes, I have.

The CHAIR — All evidence given today is being recorded. The witness will be provided with a proof version of the transcript in the next few weeks. The usual format for this is we do invite introductory statements and then we would ask an opportunity to ask questions of you.

Mr SMITH — Certainly, Chair.

The CHAIR — You are happy with that?

Mr SMITH — Yes, and I do have some introductory remarks that might assist the committee. The questions that were sent to us by the committee, questions 1 through to 7, we have examined, and we do not believe we can assist the committee too much with respect to questions 1 to 6. They are particularly law enforcement matters that relate to operational policing, and despite 41 years in policing, it is probably best left to those who are more contemporary on those particular issues. But we do believe we can assist the committee to some large extent with question 7, which relates to the information sharing environment and the role that CrimTrac plays in the law enforcement environment in Australia, if you are happy with that, Chair.

The CHAIR — Thank you. We might put you to the test a little bit in relation to 1 to 6.

Mr SMITH — I am certainly happy to answer the questions based on experience of working in a number of Australia's police forces. But what I was particularly keen to do today, when we saw the invitation, was to talk largely to question 7. We believe there is a range of matters that I think will be of quite some significant interest to the committee.

By way of background, as I said, I have been in policing now for 41 years. I started my career in Victoria Police and have travelled around Australia and finally come to rest at the moment with CrimTrac. I was involved in the creation of CrimTrac back in the late 1990s. From the point of view of question 7 of the committee's questions, it is really important to understand the policing environment in Australia and the importance of information sharing. In the late 1990s there was no formal body such as CrimTrac that dealt with information sharing across the country, and CrimTrac was a product of a meeting of commissioners and then subsequently police ministers to bring together a capability to share information.

I need to make a very important distinction for the committee, probably for discussion, between information and intelligence. Quite often these two terms are used interchangeably, but they are not interchangeable terms. If you look at the role of intelligence, that is a product that is prepared to meet a specific purpose, and so therefore you have usually some pretty specific terms of reference around the intelligence provision. So if you say, 'Look, I need to know about a particular topic', 'Here is the brief on it', so you constrain yourself to that particular topic. So agencies that provide intelligence just cannot provide a broad range of information to whoever to use in a pretty free-ranging way. The mandate for CrimTrac, however, is to provide reference information, and then the users of that reference information will value-add it in any particular way that they need to.

This is a pretty important distinction when you look at the information sharing environment in Australia. There are agencies that take information. They do what we call the value-adding role, and then they will provide that information, according to their legislative framework or mandates, back to potential users of that information. That is not what CrimTrac does. We have a library of information in the various information stores that we have and our users use that information as they see fit. That distinction is important because we do not control the way that those users will use that information. When it comes to information sharing, that distinction is critically important, because police forces will look at what they have available to them and they will make the best use of it without the constraints that often apply.

The information holdings that we have currently, and the information holdings that we potentially would have, I would like to talk about now. They do relate I think to question 7 and some of the terms of reference. CrimTrac holds the national fingerprint library. The importance of that to your inquiry, of course, is that there is one source of the truth for fingerprints in the country. If you are investigating a clan lab somewhere in Victoria and you find a fingerprint in the clan lab, it is CrimTrac that will provide the fingerprint information associated with that. So it is a very important tool for identifying people who are known to police through previous fingerprinting. You can say, 'Well, here's the national view'. There is no state view with respect to the fingerprint holdings in the country.

We also hold the national DNA library, and again, if you go into a clan lab, you take some crime scene samples, you come up with a DNA profile and you will be able to look at the national library and you get a national view of who may or may not have been involved in that particular clan lab. So with your terms of reference looking at ice, of course you look at the clan lab situation, therefore you want to know who is involved.

Associated with that we have a thing called the National Police Reference System. That is the names and the information around the people. I have spoken about the fingerprint library briefly. You have got the DNA library; they identify from crime scene information who may or may not have been involved with the particular matter under investigation. The name library is actually a much more important tool, not just when it comes to understanding about a person who you may be investigating; it is a warning system.

If the Queensland police, for example, have had previous dealings with an individual — they have got drug convictions at Mermaid Beach in Queensland — and they turn up by name in Caulfield, for example, in your electorate, the police look up the National Police Reference System. They may not have any reason to suspect that the person has previously been involved in drugs, but because you get a national view of the information that attaches to an individual they will see that this person has previously been involved in clan labs in Queensland. Their response to a particular matter can change dramatically. You might have a call to go and talk to someone at a particular address. Without the benefit of the national view you would probably just go and knock on the door, have a chat and do whatever it is that you are going to do. With the benefit of the national view of the information that attaches to that person, your response to a particular matter can change quite dramatically.

That is not intelligence per se; that is the information that police use to act upon. I would say if you are going to respond to this particular address, knowing that this person has got a history of cooking methamphetamine, your whole reaction to a particular call can be quite different.

The other thing that the National Police Reference System is very important for is that it has a thing called warnings. If a person who has been charged in Victoria absconds, fails to appear in court, and the police in Cooktown arrest the person, it is through the National Police Reference System that you would find that they have got warrants outstanding in Victoria and they are wanted. That is the service that enables those police then to know what information associates with that person.

Mr SOUTHWICK — That all sits off the LEAP database, does it?

Mr SMITH — It is connected to the LEAP database. Each police force has its own business system, LEAP being the one in Victoria. If you do a search on a name in LEAP, it will connect that name back to the national database. The information coming from the Queensland version of LEAP, which is QPRIME, that connects it together. So when the police enter the name in QPRIME, for example, from the fact that the police in Victoria through LEAP have said that there is an outstanding warrant, we make the connection at CrimTrac automatically. There is no human intervention, that is just the information readily available.

That distinction between information and intelligence is a really important distinction, because we do not know when that reference piece of information will be valuable, but we know that by having a library of that information it is valuable. We will catch 1000 people from crime scenes a week out of our fingerprint library. I do not know which one it will be today, but it will be someone. It is the same with that name library. By making those connections you get a national view of the people. The sorts of things that you will find on the National Police Reference System are warrants, information, warnings, their criminal records, all those sorts of pieces of information, and it makes an important contribution to the knowledge that police have around a particular matter.

I would like to also speak about potential. One of the things that I think is an important conversation, and it is a conversation that has taken place before a joint parliamentary inquiry here in Canberra, is about what we can do into the future as opposed to what we are doing at present. There are two conversations that are taking place nationally that I think are of significant importance to your inquiry.

One is a thing around a project called Project STOP. I do not know if the inquiry is familiar with this. It was instituted in Queensland in 2005, and it was about pseudo traffickers, or people running around shopping for pseudoephedrine. At present it is hosted by the Pharmacy Guild of Australia and has a take-up of about 60 per cent. In my opinion it is critically important that that type of information is readily available nationally.

A series of papers have been presented to commissioners at different points in time. This conversation has been going on for a while. I think it would be a real shame from my perspective as the chief executive officer of CrimTrac if we did not come to a satisfactory conversation with the pharmacy guild over this particular initiative. I was involved with the use of Project Stop information in the Northern Territory when I was an assistant commissioner there. I have seen its benefits in a number of other states in my role at CrimTrac. What we do not have at the moment is a way forward with respect to Project Stop. I am unaware of what you may or may not have been told about the future of it, but the brief I have had is that Project Stop as a pharmacy guild initiative probably needs a little bit of life support. I think it would be a real shame if we did not take some steps to ensure that that information capability was not lost to law enforcement. It is a retail initiative, and it is focused on pseudoephedrine.

Another conversation that I think needs to be had in the same context of Project Stop is a thing called end-user declarations. I am not sure if you have been briefed on these.

The CHAIR — We have had evidence from the pharmacy guild. I understand in relation to Project Stop that is not so much the guild itself, it is a couple of states, particularly with real-time monitoring. We have heard that there has been some reluctance to participate, so I can assure you from the committee's point of view that we are looking at both of those in relation to a national approach.

Mr SMITH — Certainly. The point I was going to make, Chair, if I may, is that end-user declarations suffer from a couple of weaknesses at the moment. In some states it is not compulsory to report. In some states it is not electronic data; it is manually recorded data. One of the most significant states in that regard is New South Wales, where they only manually record the information.

The weakness that comes about from not having a national view of that information and the fact that the information is voluntary and manual is that you cannot take proactive action. One example from New South Wales — and there are many of them, but this is a notable one — is the raiding of a clan lab from the central coast of New South Wales. It was only through backtracking that they found out where the implements were purchased and they could then connect that record with other people. If the police had had early access to that information from a proactive point of view, they would have known that the purchaser was purchasing stuff and there should have been a flag to keep an eye on that particular person, and then it would not have got right through to the manufacturing stage. We are not getting the benefit of that information in New South Wales in a proactive way if we are still not doing it in a national way. At least Project Stop gives you a national view of the retail sales of pseudoephedrine, but we do not have a national view with respect to the precursors that are sold from wholesalers through end-user declarations.

The interesting thing from my perspective as a manager of information sets is that end-user declarations and pseudoephedrine sales as a business process are almost identical, and it would take very little imagination to go from a Project Stop information service to the end-user declarations, because quite frankly they are the same thing. You go into a place, you buy something, you make a record of the sale and you aggregate that data for the purposes of law enforcement. I think it would be a very easy move to go from what we have with Project Stop today and then apply that to the wholesalers that are doing the sales of precursors, instruments and things like that.

Mr SOUTHWICK — Doug, do you have a view on those two areas being made compulsory rather than voluntary — as they are currently in Victoria — particularly Project Stop?

Mr SMITH — Coming from 40 years in law enforcement I have a proclivity to try to get all the information I can. The reasonableness of that is probably for others to comment on. But if you are trying to address what is a significant social problem and the pervasiveness of drugs like heroin and methamphetamine getting into Indigenous communities, I would do anything I could to try to make sure that we stamp it out. Someone can do the cost-benefit of regulation versus benefit, but from my perspective I strongly urge the committee to favourably look at the need for these services. People record sales already; they do it for their own commercial purposes. Surely it cannot be too much of a burden for a really important social issue to require that to take place.

I do not have any analysis of the number of these transactions that actually lead to a law enforcement outcome, but I think that would be an important piece of research that probably needs to be done, and you would do that as part of your assessment anyway. If you were to do a business case, for example, around end-user declarations and a national version of Project STOP for both wholesale and retail, you would look at the law enforcement outcomes. You would also look at the ability to minimise the regulatory burden that that creates on businesses, but at the end of the day you only have to look at some of the foreign jurisdictions where ice has made such an impact on communities and transfer the cost from that to the Australian situation, and I think you would do a pretty fair job on a business case to justify it.

They are the main points that I was going to make with respect to CrimTrac. We have put together a submission that we can leave with the committee. I am happy to take any questions that you may have, unless I have answered them all already.

Mr SCHEFFER — Thank you for your presentation. In that last question that you indicated was going to be the focus of your presentation, what we asked related to the fact that we thought they were sharing intelligence, but now that we stand corrected it might be information from what you have said — —

Mr SMITH — I was trying to make the distinction.

Mr SCHEFFER — No, I understand — —

Mr SMITH — In question 1 you have information and intelligence; in fact there is a difference between the two.

Mr SCHEFFER — I appreciate being set right on that; that is not a problem. We did want to look at that information sharing in connection with transnational offences. We have had evidence from previous witnesses who have spent a bit of time talking about some of the activities going on in Europe, India, China and Africa — that very complex global pattern of movement of methamphetamines. We had an Italian PhD. scholar from a university in the UK yesterday talk about what she called the mismatch in information sharing relationships between Australian law enforcement authorities and the Italians. One of our other witnesses talked about the relationships that we had with Abu Dhabi. I was just wondering if you could talk to us a bit about how our agencies work in that kind of transactional way in different jurisdictions.

Mr SMITH — Certainly. Firstly, the mandate for CrimTrac is just a national mandate.

Mr SCHEFFER — So this is an inappropriate question about transnational?

Mr SMITH — Not particularly. The current mandate of CrimTrac is evolving. In the area of cybercrime, for example, I now have a very clear mandate to have a look at information sharing in a number of jurisdictions, including Europol, Interpol and things like that. I think one of the first things to be conscious of is volume. Any information may not in fact be useful, so you have to really target the information you get and the way that you use that information, otherwise it actually becomes a burden rather than a bonus.

If you look at the operating model of CrimTrac, it is about information that provides an opportunistic benefit. As I said, it is a library of information as opposed to targeted intelligence. My colleagues at the crime commission and at the Australian Federal Police have a much broader mandate with respect to international crime — transnational crime — and of course they have a much more targeted focus. What you do is you actually look very clearly at why you need information, otherwise you will just get swamped with volume and it will not be of any benefit whatsoever.

However, from an information sharing point of view, the more that you can automate and aggregate information so users can benefit from that is a very important topic. I have recently been working with Europol, in the area of cybercrime in particular, on information sharing. The thing that we need to make sure that we have got the ability to do is to share. I think it is an unfortunate truth at the moment that we are culturally bound. We usually share with people that have like systems, and we usually share with people that we can actually communicate with. It is no surprise that information from jurisdictions where there are language barriers, and where there are cultural barriers with respect to the way that they operate their judicial systems, we do not share well. That is no surprise, because if you cannot communicate, you cannot share information.

When you look at the need to share, no. 1, it is around the standards that are associated with information. From a CrimTrac point of view we are entering into agreements to share information around criminal histories overseas. No. 1 for me is the ease with which we can communicate, so it is the standard around the name and it is the way that the data is presented, the systems and the amount of automation that can be put into it to in fact make it possible for the users to get that data.

We are also working with the Australian Federal Police to get Interpol warning notices available to police. At the moment an Interpol warning notice of a particular kind, drug traffickers or whatever, is usually only presented to police users if they ask. Shortly it will actually present that information through the NPRS, so a police officer who inadvertently, accidentally or unwittingly has contact with someone, our system with fingerprinting and name matching will be able to say, 'Hold on, that person is actually known overseas through an Interpol red notice'.

So we are moving into that area, but it has not been a priority of CrimTrac, because frankly we have got enough work to do just trying to share the information nationally in the first instance where we get the greatest benefit.

Mr SOUTHWICK — A couple of questions, firstly around unexplained wealth. I am interested to know where you might see CrimTrac being able to assist when it comes to unexplained wealth legislation and laws.

Mr SMITH — With respect to unexplained wealth, we probably have not got much of a role to play at all in that area. Our colleagues from AUSTRAC have a significant capability there, and there would probably be little benefit in duplicating it.

Where I have had contact with John Schmidt over at AUSTRAC is in the area of warning notices. If you have got someone involved in the movement of funds, it is about getting the warnings that are associated with that person to populate the database, the NPRS in particular, and again it comes back to the distinction between targeted intelligence and opportunistic information residing within the NPRS.

We have had conversations about putting that data into the CrimTrac database as a warning to say, 'This particular individual is a known money trafficker, a known money launderer', if for no other reason than that just gives an alert to police who are not part of a particular targeted investigation. That is probably the extent of it from our perspective.

Mr SOUTHWICK — That is fine, and cybercrime, which you alluded to before, in particular has some activity around social media and criminal footprint intelligence gathering of people using Facebook and the like for trading illegally.

Mr SMITH — I was thinking of a couple of other websites, one of which was recently closed down. CrimTrac has got a very extensive mandate with respect to cybercrime, and the starting point for any conversation is around your definitions, so we adopt the definition from the national cybercrime plan. Our responsibility at this point in time is to provide the cyber online reporting network, the ACORN. That cyber online reporting network will enable anyone, either anonymously or by identifying themselves, to make a report of cybercrime.

The metrics that we have looked at, having regard particularly to the Europol cybercrime reporting network, indicate that predominantly more than 50 per cent will be related to paedophile activity; a very large proportion will be the identification of websites that are involved in inappropriate sales and trafficking. If you look at the sorts of websites that are involved in selling drugs in particular, we will have the ability to take the reports — and in Europe a large number of them are anonymous reports — on inappropriate websites and that sort of activity.

That capability will be available from the third quarter of this calendar year, probably some time around July or August it will go live with that. What that will enable us then to do is to automatically generate reports to police forces that have a reason through the reporting rules to get that information. We would anticipate that in the area of unlawful drug traffic probably about 10 per cent of the reports will be related to that. There is a perception that it is largely fraud, but the experience in Europe is that it is not, it is paedophile activity, the sale of paedophile images and a large amount of trafficking in things like guns and drugs. And then you get down into the online fraud, which is probably more often associated with cybercrime.

Mr SOUTHWICK — There is just one last thing, and this is the question all governments like to know the answer to. With the two database tools, Project STOP and end-user declarations, what sorts of costs would be involved — ballpark?

Mr SMITH — I have been very remiss in that regard; I should have identified the business model of CrimTrac. It really is an important point for governments, both federal and state. CrimTrac was the product of a desire of commissioners to deal with an information problem. Ministers agreed to it, and when CrimTrac was created there was seed funding provided by the commonwealth government, but it is run by commissioners and by ministers.

We do not ask for any appropriations; we actually fund all of our activities without worrying the treasurers and the finance ministers of the country. We have the responsibility for selling the criminal history checks that businesses need for their vetting of potential employees. That money goes into a special account which is run by CrimTrac. At present it costs me about \$70 million a year to run CrimTrac on an annual basis, and I have revenue that exceeds that expenditure each year. We then make a provision within the special account for future investment, and if the CrimTrac board and ministers at the ministerial council were of a mind to mandate work on Project STOP and end-user declarations, the business case would indicate the cost. I would expect that it would be less than \$10 million, without trying to get too detailed — you always get into trouble when you have a guess around those costs. But that being the case, there is more than sufficient provision in the CrimTrac special account to cover that. We have presently got over \$112 million to invest in projects like this, and if there were a collective mind and will of police ministers to do that, we could do that from within the special account.

Mr CARROLL — Thanks, Doug, for your information and advice. The committee has been going all around regional Victoria, where ice seems to be an issue. We have been talking to a lot of local police — and this is a question on your background as well — and one of the issues that has come up a few times has been a police resourcing issue in the sense of forensics, DNA. If the local police find a car boot laboratory making crystal meth, for them to then get the fingerprints and the DNA evidence they often have to do what is sometimes a 6-hour round trip to the forensics centre in Melbourne and then back and then do their law enforcement at the regional level.

Obviously we do not have an unlimited budget to set up forensic medicine centres all over regional centres, but with your background and all your experience in the states and territories, is there a better way that we could be doing the forensics, the fingerprinting and all those things to get it to CrimTrac quicker and also help police in remote regional areas?

Mr SMITH — I will have to preface my remarks by saying that I am not completely familiar with every aspect of the business path adopted in Victoria, and I would not like to comment in too much detail about things that could be improved. I could speak generically. Largely, based on my experience in Queensland, they have a thing called the forensic register. This is a laptop tool which does not require any special expertise. They do not use fingerprint experts in the field, they use crime scene examiners. In some cases it is just a police officer who is reasonably well trained in the field.

Put yourself out in Longreach: you are a police officer in Longreach and you find a clan lab in a shed outside town. The first thing about fingerprints is that the way that we deal with them they are only an image. There is no magic these days to a fingerprint. So long as you can develop the fingerprint in situ with dust or superglue or something of that nature and you can take a photo of it, we are good to go. What they do in Longreach is get the image, they load it up into the laptop computer and then over the 3G network it makes its way to Brisbane and then straight into the national database. One of the most timely examples I could give had an unfortunate outcome. You might remember that a little over 18 months ago a fellow from northern New South Wales drove to Queensland to Robina, killed his wife and one of his children, and then drove back to New South Wales. The police attended the scene at Robina, and within an hour they had identified, through the fingerprint, who he was. We had identified from our databases the car that he was most likely driving. Unfortunately he had taken the other child back into New South Wales and killed her in the car.

The point was that they were able to get that fingerprint from the scene to our library and back to them within the hour to identify who he was. That is not an unusual turnaround. I know that at Upper Coomera we have been developing fingerprints for police there and they are getting home before the crooks. They have been waiting at the door when the crooks have arrived home with a boot load of stolen goods because we have such a quick turnaround.

Based on those examples, I am pretty comfortable in saying that an assessment of your capability in Victoria might lead to efficiencies that can get a quick turnaround, without the need to drive to Melbourne. I am conscious of efforts that Chief Commissioner Lay has been making in Victoria to

improve the service, but it would be completely inappropriate for me to comment on the internal business processes in Victoria Police.

The CHAIR — I had a few questions, I must say, but given that you have declined to respond to questions 1 to 6 — —

Mr SMITH — I am willing to entertain the questions. I was just trying to focus my comments on question 7 because I thought that that is where I could assist the committee the greatest.

The CHAIR — On that basis and knowing that you have made a written submission, if we require more information than is in the written submission or in some of the questions we have not posed to you verbally, I am wondering if you might respond to those.

Mr SMITH — After 40 years in police work, I would be more than happy to do whatever I can to deal with the problem, because it is not going to get any better. If there is anything I can do to assist, I would be more than happy in that regard.

The CHAIR — Thank you. Do you have a closing statement you would like to make?

Mr SMITH — I do not think so, but I will just check with my colleagues to make sure that I have covered the points I should have.

Mr SOUTHWICK — I might ask a general question.

Mr SMITH — Just before you do, if I may, as the assistant commissioner in the Northern Territory responsible for crime, I will comment on one of the things that I think is really important when you talk about drugs in country areas and in Indigenous communities. I witnessed the flow of heroin into Indigenous communities in the Northern Territory. It was a really depressing thing that occurred. It was largely coming out of Sydney, and the trafficking of the heroin was incredibly well organised. It was to get people addicted, and then the criminality followed it. It was a really scary thing to follow. If you look at what is now happening in the Northern Territory and remote communities in Queensland with respect to methamphetamine, you see that the same thing is happening.

In the past we have had a lot of issues in Indigenous communities that are quite frightening, such as petrol sniffing and things like that. As a professional in this area I am very concerned to see what has happened in the past. When you look at the nature of methamphetamine addiction and the damage that it is likely to cause, I think we really have to have a pretty forceful action in this regard, otherwise we are going to have consequences we are going to find very, very hard to deal with.

Mr SOUTHWICK — I will go back to something that you are able to answer, specifically around the international cooperation. I know that you are flat out working nationally, but the evidence that we have had thus far is very much that there is a lot of international activity, with drugs flowing in and out of all different jurisdictions, with places used for transit and multiple parties involved. In order to really focus on the big catchments, what other strategies could CrimTrac have or be assisting with to expose that sort of international racketeering?

Mr SMITH — I will go back to the distinction that I was making between information and intelligence. There are more than 60 000 police officers in Australia. If you choke information down to particular segments of law enforcement in the country, you do not harness the benefits that perhaps 60 000 police could bring to the table. I look at the large distinction between information and intelligence and I say, 'Look, as a professional in this area there are untold benefits with intelligence and the targeted use of information'. But at the same time if you want to get the 60 000-strong police force to work on a particular topic, you have to give them the information upon which to act. So I think at some point in time we need to recognise the benefit, if you like, of this library of reference information and say, 'We don't know if this information, whatever it is, may be of benefit, but we need to get it out there so people can use it appropriately and as they see fit'.

From my perspective as we develop the role and functions of CrimTrac into the future, we already have an architecture and a blueprint looking forward as to what we can deliver. We all have a focus at CrimTrac, given to us by the board I hope, where we look at new information systems. I think that is the place where you take that international information that you cannot actually focus on through an intelligence activity but you then make that available to police officers more generally. So information about the nature of trafficking, the sorts of property that you need to be looking for and those sorts of things need to be made more broadly available, I think.

Mr SOUTHWICK — If I turn that around a little bit, where are we in terms of our information gathering compared to other jurisdictions in the world? Would we be internationally recognised and seen as being able to gather the sort of information that others are envious of? Could we have a role in equipping other jurisdictions that have the same sorts of problems as we do with the know-how to be able to set up similar sorts of CrimTrac information gathering systems in their jurisdictions?

Mr SMITH — If you were to compare us with New Zealand, because they are not a federation the world is pretty good over there so they just have the one source of the truth. In the United Kingdom you have 43 police forces in England and Wales; they are pretty disorganised. They have systems where they are trying to share. Even in such a small country they have difficulty. We are actually doing pretty well.

The issue is that there has been an information explosion. Obviously there is a huge appetite for information, and we are always behind the game. That is just the nature of the beast. If you recognise the fact that Australia has had one of the most advanced national fingerprint systems for a long time, we are in a pretty good place in that area. With respect to DNA, the lack of harmonisation of laws is a problem. In some jurisdictions you get a much greater benefit from their DNA laws than others. Quite frankly the laws in Queensland from a law enforcement perspective give us a better outcome than what they do in a number of other states, including Victoria.

The advantages over things like familial searches that are possible in some jurisdictions and not others need to be recognised if you are looking at enhancements that could be made from a legislative point of view there. In the more general information sharing area and the aggregation and analysis of data, I think everyone is trying to cope. I do not know whether there is any exemplar where you would say, 'They're doing it much better than us'. If you look at the volumes in the United States, just trying to get value out of those volumes is always a problem. I think we are doing pretty well. I think we can do a lot better, but that said I think we are doing pretty well.

Because of the nature of the business I do not know how much more we could do without a huge injection of funds and effort, and of course then you have to balance competing interests. I hope I have answered that satisfactorily. It is a very difficult question. You can always find things around the world that you would love to emulate. Then you look at your work program and the appetite to do things, and you take a reality check.

The CHAIR — Given there is so much information now being shared within the jurisdictions and building on the work that you are doing with CrimTrac in relation to community confidence in security of information, I am reminded of the LEAP database, where there have been a number of concerns raised about access. Given you are providing much more information on a national basis on individuals, is there a general reluctance to information share based on perceived concerns around security?

Mr SMITH — I will make a couple of points. Number one is from a CrimTrac perspective and my perspective privacy is a very important thing. I have always made the point that if there are concerns about privacy, that goes to the trust and reputation of the organisation, so I am very keen to make sure that the protection of information is there. When we talk about privacy, I do not associate that with anonymity. In a lot of quarters, people make the leap from privacy to anonymity. I think that is too big a leap. Unfortunately in some of the conversations people want to remain completely anonymous in the information world, which is unrealistic.

With respect to the access to data, your weakest point is the user. As soon as you have a human with information, that is when you are at your weakest point, not the systems. I do not want to put a public challenge out there, but we have recently tested our systems, as we often do, to see whether they can be hacked into, and I have a very high degree of confidence that we are very secure. However, as I said, the weakest point with data is the user. The examples that you referred to, Chair, are probably examples where the user has taken information from a system and misused it. That is always going to be our weakest point. That is a matter of discipline and proper auditing.

Everything that we do inside CrimTrac has an audit log, and we never lose those audit logs. I can go back and say, 'This particular police officer in this state accessed this piece of information' so then the internal investigations areas of police forces can access it and we provide it when they ask. We know what is being looked at. I do not know if that answers your question. I have some notes here.

The CHAIR — Jane is nodding, which is a good sign.

Mr SMITH — It is a good sign, Chair; I got that right. This is probably getting into too much detail, but there is a thing called chain computerisation. As we move forward, we will be implementing policies inside CrimTrac. What we are talking about there is at the centre, which is where CrimTrac is, you have core data and your risks with core data are not as high as the data attached. So if you name data is what the centre holds, then that is not really that risky; it is what is attached to the name. You do not take the data from the various data sources; you connect with that data. Then it is only by user requirement that they can touch the data. In the European example, they do not bring to the centre all the information; they have a cache or core data at the top and then you access the attached data as you need to and as you have authority to. So if you want to go into data that is held by the Dutch police, firstly you have to have a reason. You do not take that data to a big database in the centre where the risks are high; only a user with the right to access goes to the data through the top layer into the data and that preserves sovereignty. It helps to protect privacy to a higher degree and it also ensures accuracy, because if you take data from one source and put it in another source, keeping those two data elements the same is a problem.

As we move forward with new information capability, that is an area that we will have to deal with. We have a plan that we will soon be taking to the CrimTrac board to make sure that we have that conversation. I hope I did not go too far from your question.

The CHAIR — It was a legitimate question on the basis that I assume as we progress there will be more information required from individuals through end-user declarations, real-time monitoring, Project Stop or other information requirements.

Mr SMITH — Certainly. We operate very closely with the requirements of all jurisdictions, because each of them have their own sovereign rules. With respect to Victoria we are very conscious of the rules that the commissioner for law enforcement data security puts on the chief commissioner. Every one of them has something unique, and they are part of our operating environment.

The CHAIR — Thank you very much.

Mr SMITH — Thank you, Chair. If I may, this is our submission. As I indicated, I am more than happy to respond to any other questions you might have.

The CHAIR — We note that you are happy for that to be tabled. Thank you.

Witnesses withdrew.