REPORT ON PROCEEDINGS BEFORE

STANDING COMMITTEE ON LAW AND JUSTICE

ROAD TRANSPORT AMENDMENT (NATIONAL FACIAL BIOMETRIC MATCHING CAPABILITY) BILL 2018

CORRECTED

At Jubilee Room, Parliament House, Sydney on Wednesday 7 November 2018

The Committee met at 2.06 pm

PRESENT

The Hon. Natalie Ward (Chair)

The Hon. David Clarke
The Hon. Scott Farlow
The Hon. Adam Searle
Mr David Shoebridge
The Hon. Lynda Voltz

The CHAIR: Welcome to the inquiry of the Standing Committee on Law and Justice into the Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018. Before we commence, I acknowledge the Gadigal people who are the traditional custodians of this land. I also pay respect to elders past and present of the Eora nation and extend that respect to other Aboriginal persons present or listening to this broadcast. Today the Committee will be hearing from representatives of the NSW Information and Privacy Commission, NSW Council for Civil Liberties and representatives from the New South Wales and Federal governments.

I will now make some brief comments about the procedures for today's hearing. Today's hearing is open to the public and is being broadcast live via the parliamentary website. A transcript of today's hearing will be placed on the Committee's website when it becomes available. In accordance with the Legislative Council's *Guidelines for the Broadcast of Proceedings*, while members of the media may film or record Committee members and witnesses, people in the public gallery should not be the primary focus of any filming or photography. I also remind members of the media that they must take responsibility for what they publish about the Committee's proceedings. It is important to remember that parliamentary privilege does not apply to what witnesses may say outside of their evidence at this hearing. I urge witnesses to be careful about any comments they may make to the media or to others after they have completed giving their evidence. Such comments would not be protected by parliamentary privilege if another person decided to take defamation action. The guidelines for the broadcast of proceedings are available from the secretariat.

Due to the very short time frame of this inquiry, no questions will be taken on notice. Witnesses will be asked to provide their answers today. Witnesses are advised that any messages should be delivered to the Committee members through the Committee staff. To aid the audibility of this hearing, I remind both Committee members and witnesses to speak into the microphones in front of them. In addition, several seats have been reserved near the loudspeakers for persons in the public gallery who may have hearing difficulty. I ask everyone to turn their mobile phones to silent for the duration of this hearing. I now welcome our first witnesses: Ms Tydd, Ms Gavel, Dr Lynch and Ms Falstein.

ELIZABETH TYDD, NSW Information Commissioner, NSW Information and Privacy Commission, sworn and examined

SAMANTHA GAVEL, NSW Privacy Commissioner, NSW Information and Privacy Commission, sworn and examined

LESLEY LYNCH, Vice President, NSW Council for Civil Liberties, affirmed and examined

MICHELLE FALSTEIN, Convenor, Privacy Committee, NSW Council for Civil Liberties, affirmed and examined

The CHAIR: Would any of you like to make a brief opening statement?

Ms GAVEL: Ms Tydd and I both wish to make an opening statement, but I have kept mine fairly short so that everyone can speak. I am pleased to have this opportunity to appear at the inquiry of the Standing Committee on Law and Justice into the Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018. The Information Commissioner and I have made a written submission to the Committee about the bill. We note that the policy content of the bill is to improve the ability of government agencies to share and match facial images to prevent the creation and use of fraudulent identities, which in turn supports law enforcement, border management, national security and service delivery outcomes. The Information Commissioner and I support in principle these objectives, subject to appropriate privacy and security controls.

Any use of a biometric system to collect and use personal information must be done in a way that is reasonable, relevant and not excessive in relation to the purposes for which it has been created. In particular, it is critical to create a strong privacy protection framework for any project involving the use of biometric information. The NSW Information and Privacy Commission is actively engaged in the promotion of rights and protection of privacy. The commission has been consulted by the Commonwealth and New South Wales governments in respect of the development of the national facial biometric matching capability. I and the previous NSW Privacy Commissioner have been involved in this cross-jurisdictional engagement. This engagement has enabled privacy considerations to be taken into account from the very earliest stages of design and development of the capability.

This bill is part of broader national reforms and sits alongside the Commonwealth's Identity-matching Services Bill 2018. It follows the commitment made by the States and Territories at the Council of Australian Governments and, as a result of that commitment, on 5 October 2017 an Intergovernmental Agreement on Identity Matching Services was entered into by the Commonwealth and the States. The agreement makes it easier for security and law enforcement agencies to identify people who are suspects or victims of terrorist or other criminal activity, and to prevent the use of fake or stolen identities. Overall, the Information Commissioner and I consider that the bill operates within the framework of relevant legislation and the State's privacy regime, including the requirement for legislative authority to collect, use and disclose facial images and other personal information.

Ms TYDD: My opening statement will also be very brief. I am pleased to have this opportunity to appear before the Committee in respect of its inquiry into the Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018. The Privacy Commissioner and I have made a written submission to the Committee about the bill that notes the policy context of the bill and the Information and Privacy Commission's [IPC] ongoing engagement at a Federal and State level with respect to the National Facial Biometric Matching Capability. The Privacy Commissioner and I are committed to the promotion of information access and privacy rights and see our partnering with agencies and governments as a means to further those aims.

Our written submission to the Committee touches on information sharing and the public interest. Those submissions identify that under the Government Information (Public Access) Act [GIPA] and in information governance generally, factors including national security, law enforcement and privacy, should be considered to inform any decision regarding the management of information. Controls, including custody and access arrangements, are also significant factors requiring consideration. Having regard to the object of the bill highlighted by the Privacy Commissioner, the public interest may favour information release to other government agencies for the purpose of law enforcement and security with appropriate safeguards built into the scheme.

The Privacy Commissioner and I consider that the policy objectives of the bill, which involve information sharing between agencies of facial images for the purpose of law enforcement and national security, among other things, together with appropriate controls informed by ongoing consultation, may serve the public interest. Additionally, as an entity, the IPC commits to a continuation of support for and input into that extensive consultation process to achieve the optimal outcomes for citizens and agencies.

The CHAIR: The Committee appreciates the brevity in your statements and we thank all of the witnesses for providing written submissions on such short notice.

Dr LYNCH: I will make a shortish opening statement. What I want to do is to talk a little bit about our approach to the submission. The road transport amendment [RTA] bill after all is very short. It is a minimalist bill. It does not say a great deal. We have responded with historical and contextual considerations and reflections and broader concerns about the development and the future implications of the whole national identity matching database activities and services. Most of our comments relate to provisions and issues that are not mentioned in this bill but which we consider to be very centrally relevant to this bill. We do this in the hope that consideration of the broader context and the likely long-term implications will encourage the New South Wales Government and our Parliament to give very close consideration, much closer than is apparent, to the protections for both privacy and the maintenance of a healthy democratic society before passing this bill.

A very powerful database is being built and Civil Liberties is not, in principle, opposed to national consolidation activities which make identity checking faster and more efficient. That is not, and has never been, the issue. However, there are dimensions to it which do have bigger, long-term implications and if access is not tightly limited around all of those services in that national—we can call it capability if we like, that is how the New South Wales bill speaks about it, the capability—

Mr DAVID SHOEBRIDGE: Everybody is now referring to it by the evil title of "the capability".

The CHAIR: Thank you, Mr Shoebridge. I would like to hear the opening statement.

Dr LYNCH: I know, but I think that is also partly a young persons' social media and television joke that is running. Our basic position here is, because of the implications, if access is not tightly limited this whole enterprise does have the power to seriously erode some of the things which are very important in our democracy. The transformational element in the overall surveillance agenda is then enhanced capacity for close to real-time matching of unidentified facial images against a growing and eventually pretty large national database. The sources for these images, as we know, are many. CCTV is almost everywhere we go now; almost everybody has their own phone in their hands most of the time, their iPhone and so on and so on. This delivers a technical capacity for real-time mass surveillance of public gatherings as well as the terrorist and other public safety incidents.

We are assured, and I listened to the Privacy Commissioner's comments, we are certainly assured at the national level by Government and assured by the New South Wales Attorney General that the system's capabilities will not be used for general mass surveillance. But, given history and given the technological capability that is now available, it seems unusual or unlikely that the usual syndrome creep will not continue and it is hard to believe that it will not lead to pressure in the not-too-distant future for this capability to be used in many contexts and for many reasons. As we point out in our submission both on this bill and to the Commonwealth in our larger submissions, this brings with it a real threat to anonymity. But the more concerning dimension of it is the attendant chilling effect on the freedoms of political discussion, the right to protest and the right to dissent. We think these potential implications should be of concern to us all.

So for these broad reasons, it is important that all aspects of the national database and the identity-matching and identification capabilities are very tightly controlled to give maximum protection to the privacy of non-suspect individuals and to the robust privacy safeguards and robust compliance framework that we have been promised in numbers of contexts both in the agreement and in the Attorney General's second reading speech at both the New South Wales and the Commonwealth level. The Integrated Academic Information Management Systems [IAIMS] agreement had reasonable protections built into it, but, as we argue, the Commonwealth bill is drafted expansively re access and benchmarks and constraints and various other aspects and is in many provisions inconsistent with the IAIMS.

The CHAIR: Dr Lynch, I am going to give you two more minutes, if you do not mind. We must move to questions shortly.

Dr LYNCH: Yes, I can do that, I think. The Parliamentary Joint Committee on Intelligence and Security [PJCIS] has not even completed its inquiry into the broad package and there is, of course, no Commonwealth Act yet, so none of us knows what amendments will be proposed or passed in that bill. The RTA bill is silent on these contentious issues except that it does, I think, lessen the New South Wales privacy protections in section 271A (3). I will summarise by saying a big burden in terms of the appropriate protections has been placed on the agency participation agreements. As far as it is publicly known—the commissioners might have been involved in this—as far as we know, that does not exist yet. So nowhere is there anything that we can look to that addresses either the inconsistencies with the 2017 agreement or that addresses the numerous weaknesses that many of those who responded to the Commonwealth framework bill have drawn attention to. So it is in that context that we make the kinds of comments that we made in our submission. Thank you.

The CHAIR: Thank you. Ms Falstein?

Ms FALSTEIN: I have got nothing to add to Dr Lynch's remarks.

Mr DAVID SHOEBRIDGE: One of the principal concerns that has been raised with my office is the ability for this information, once it has been gathered together in the Capability, to be shared with private entities, corporations and the like. Ms Gavel, I did not hear you address that in either your opening submission or in your written submission. What do you make of the proposition that information that is currently protected with strong privacy protections in the form of photographs and details on New South Wales driver licences are going to be thrown into this big capability and then able to be accessed by private corporations?

Ms GAVEL: I understand that entities will only have access to the system through participation agreements and that there are some significant restraints on private sector access to the system. I am just trying to find where they are.

Mr DAVID SHOEBRIDGE: I might help. The Minister makes a rule under clause 7 (2) of the Commonwealth bill and then access is granted under clause 7 (3) (b).

Ms GAVEL: But there are requirements in place for the Minister to consult with the Privacy Commissioner and the Human Rights Commission for law changes as well in the Act—the Commonwealth Privacy Commissioner.

Mr DAVID SHOEBRIDGE: So there is a consultation obligation, but that is no protection; that is just a consultation.

Ms GAVEL: But my understanding as well from the consultation that I was involved in earlier this year is that if private access were to be given, and that is not a given at the moment, it would be on the basis of a yes/no response from the system; they would not be receiving information from the system. That is my understanding.

Mr DAVID SHOEBRIDGE: But there are none of those protections in the Commonwealth bill.

Ms GAVEL: No, but the Commonwealth bill will also be underpinned by governance documents as well and other material such as the privacy impact assessments that have been done on the system.

Mr DAVID SHOEBRIDGE: But if a future Minister, such as the current Minister, Peter Dutton, if they consult with you or they consult with your Federal counterparts, they do not agree with their provisions, they can make whatever rules they want regardless of the import of that consultation.

Ms GAVEL: At the same time, any consultation on this would enable both the Commonwealth Privacy Commissioner and commissioners from jurisdictions to consult on these issues and, as we have done from the start of this process, which has been ongoing for a number of years, we have insisted that it be a privacy-by-design process from the start, with privacy protections built in, and that process will be ongoing.

Mr DAVID SHOEBRIDGE: But if it is going to be a yes/no for private entities, if that is your understanding, why is none of that in the Commonwealth bill?

Ms GAVEL: The Commonwealth bill is the overarching framework, but it is also going to be underpinned by governance and other requirements, including the participation agreements between the States and the Commonwealth. None of this information is settled yet. As you know, the Commonwealth bill is still in Committee.

Mr DAVID SHOEBRIDGE: So how can you be satisfied that there are adequate protections when the Commonwealth bill has not even passed? We are handing it over to an unknown entity, yet you are giving the sign-off from the Privacy Commissioner's perspective in New South Wales. We have not even seen the Commonwealth legislation.

Ms GAVEL: Because I have also seen some of the documentation underpinning the system and have been able to have input into that documentation along with other State and Commonwealth Privacy Commissioners.

Mr DAVID SHOEBRIDGE: I find it really surprising that the Privacy Commissioner in New South Wales is signing off on New South Wales entering a Federal scheme that has not even been legislated yet. It seems more wing and a prayer than considered advice.

Ms GAVEL: My role is not to sign off on the scheme; that is being done through the intergovernmental agreement between Commonwealth and State first Ministers. My role is to ensure that the privacy protections are in place, that the system has been put together through privacy-by-design principles and that there are appropriate and robust safeguards in the system to safeguard privacy and security.

Mr DAVID SHOEBRIDGE: When it comes to private individuals, the only safeguard that I can see is that (a) it has got to be the subject of a future rule-making by the Minister, and (b) the only actual safeguard is that contained in clause 7 (3) (b). Do you agree with that? Are you aware of clause 7 (3) (b)? I am asking you about clause 7 (3) (b).

The Hon. SCOTT FARLOW: Of the Commonwealth Act?

Mr DAVID SHOEBRIDGE: The Commonwealth Act.

The Hon. LYNDA VOLTZ: Which is the overarching legislation.

Mr DAVID SHOEBRIDGE: Which is where we are handing information over to. You cannot say this is okay from a State perspective unless you understand where it is going. So I am asking you about the scant protections in 7 (3) (b) of the Commonwealth bill.

Ms GAVEL: Yes, but the Commonwealth bill provides the overarching framework for the system. There will also be governance arrangements underpinning the system as well.

Mr DAVID SHOEBRIDGE: I am asking you about the statutory protections in clause 7 (3) (b).

The CHAIR: The witness has answered that question three times.

Mr DAVID SHOEBRIDGE: Are you aware of the very limited statutory protections in the Commonwealth bill?

Ms GAVEL: That is not my understanding from the consultations that—

Mr DAVID SHOEBRIDGE: I will read it to you to help. The condition that needs to be satisfied before information in the capability can be handed to either a local government agency or a private entity is that the individual in respect of whom any of the information is gathered has given consent to use and disclose "... for the purpose of verifying the individual's identity the identification information about the individual that is included in the request ...". That is it—consent. Are you satisfied with that?

Ms GAVEL: I understand that the Commonwealth bill has a number of safeguards which are set out in the explanatory memorandum. One of them is limiting the use of particular identity matching services to only those organisations and agencies that have a reasonable need to use them and for specific purposes.

Mr DAVID SHOEBRIDGE: Stopping you there, "reasonable need" is so extraordinarily broad, you could not be satisfied with that protection, surely? A 7-Eleven outlet may have a reasonable need to know the identity of anyone who walks in because they may want to check their identity. "Reasonable need" is not a protection.

Ms GAVEL: I am concerned that we are now going to issues of the Commonwealth bill which is still in committee in the Commonwealth. That has not been finalised yet and I am not able to comment on because I have not seen the final form of the bill.

The CHAIR: The witness has been asked to comment on the New South Wales bill.

Mr DAVID SHOEBRIDGE: You can only understand the impact of the New South Wales bill if you know where the information is going. The only purpose of this bill in New South Wales is to send information to a Commonwealth scheme that is regulated under the Commonwealth bill.

Ms GAVEL: Yes.

Mr DAVID SHOEBRIDGE: If you are not satisfied by the protections in the Commonwealth bill, how can we be satisfied that the privacy of New South Wales residents, which is your primary concern, is being protected? I do not understand.

Ms GAVEL: The Commonwealth bill is subject to the Commonwealth privacy scheme and oversight by the Office of the Australian Information Commissioner and information going there is subject to the privacy principles at the Commonwealth level.

Mr DAVID SHOEBRIDGE: Those privacy principles are read down to the extent that there are these express provisions contained in the bill. I am going to ask you again, are you satisfied with the concept of bundled consent being an adequate protection before individual's private information is handed over to private corporations? Are you satisfied with bundled consent being the protection?

Ms GAVEL: I am not aware that is the way the system is going to work.

Mr DAVID SHOEBRIDGE: I just read you clause 7 (3 (b).

The Hon. SCOTT FARLOW: Ms Gavel gave an answer that referred to the privacy legislation.

The CHAIR: The witness has attempted to answer.

Mr DAVID SHOEBRIDGE: Ms Gavel, you have not addressed the concept of bundled consent in clause 7 (3) (b). We all know what that means. That is the eight pages of closely typed font that you press "okay" to when you want to access telecommunications services, you want to get your car serviced, or you want to stay at a hotel. The bundled consent will be sufficient to grant private corporations access to private information under the capability. Are you satisfied with that?

Ms GAVEL: I do not understand that is the case. I think there are far more protections than someone signing a document like that. As you know, I have concerns about bundled consent and that is something my office is looking at at the moment.

Mr DAVID SHOEBRIDGE: How can you be satisfied that bundled consent will not be the consent that is sufficient to satisfy clause 7 (3) (b) of the Commonwealth bill?

Ms GAVEL: Through the ongoing opportunities I have had to consult with the Commonwealth on this and my understanding of the system through those consultations, and also the ongoing consultations that will happen. As I said, the system is not in place yet; there is still consultation that needs to occur. At this stage there has already been a lot of consultation and I am aware of the concern that I and other privacy commissioners have to ensure it is a safe and robust system where people's most personal information is kept safe.

Mr DAVID SHOEBRIDGE: Dr Lynch, can I ask you about the legislative protections? Not the statements but the legislative protections.

Dr LYNCH: I will refer to my colleague for the details. We are not opposed to a capability which does what it sounds like it is going to do when the Prime Minister and various premiers and ministers have spoken about it. That is, the bringing together of databases into several departments, but with the Home Affairs agency having the overall control, in so far as what it is doing is speeding up the capacity for people to be able to check identities. That is fine. We have a caveat about that like every sensible person should have, which says the more big databases you have got the more the honey pot syndrome works. We have seen so many times in the last couple of years how vulnerable government agencies—not just ours, many—are to being done over. I come from a household which has just had an identity theft from a database being done over. We are not worried about that.

The new element that makes it big stakes is the transformation in terms of the capacity for almost real-time identification of an otherwise anonymous individual against a large databank. Now, if we are talking a terrorist event, a public safety threat event, I do not think anyone much would disagree with that. If we are putting into place a capability which gives government the capacity for real-time surveillance, it is big stakes. And it is big stakes not just in terms of people's privacy; it is big stakes in terms of the nature of our democracy. I think it is a pretty incontrovertible historical fact that if you have that kind of surveillance you have a profound chilling effect on people's willingness to go to a demonstration if you know you could be picked up.

All the commentary you heard a month, two months ago when the newspapers were running coverage of—oh, my gosh, look what the Chinese can do—they can look into a mass gathering where there are 500,000 people and they can target that group of people and they can know all sorts of stuff about them in no time at all. We are at the beginning of that process under this Commonwealth legislation. I find it really strange that the New South Wales Government—and a couple of other States as well—is willing to move ahead with such a minimalist piece of legislation. This bill does the absolute basics of authorising the authority to be able to participate. It does a few things we do not like. But we do not know what the Parliamentary Joint Committee on Intelligence and Security [PJCIS] is going to say. There are a lot of really concerned and critical views, including from the privacy people, as I remember correctly, about that bill. We do not know what is in the agreements.

The CHAIR: We might leave it at that. We have taken your point on that.

The Hon. LYNDA VOLTZ: Ms Tydd, in regard to your submission, do you have any concerns around the safeguards?

Ms TYDD: There would be a number of issues that I would like to cover in that response. The operation of the scheme, as I understand it in its current development, reflects some of the existing principles that apply to access to information, and they include consideration of matters such as national security, law enforcement and privacy. In that regard there is an alignment of those principles both through the proposed approach of the Commonwealth scheme but also within both privacy legislation and information access legislation at a State level. There are provisions in the Government Information (Public Access) Act, to turn to my jurisdiction, that recognise that information held by a government agency may be applied for by way of access from a citizen and in doing so

agencies would have regard to the existing factors against disclosure of that information—for example, release to a citizen making an application that are provided under the Government Information (Public Access) Act. Some of those factors I am sure are well known. They include privacy; they include law enforcement. There are of course carve-outs, exemptions, in relation to security.

The Hon. LYNDA VOLTZ: Ms Tydd, those provisions are against the release of information?

Ms TYDD: That is correct. I thought your question may have been going to if this information was released more broadly other than for the purposes that were articulated in the bill and the objects of the bill in terms of national security law enforcement—those provisions. I was answering the question with respect to that.

Mr DAVID SHOEBRIDGE: It is much broader than that.

The CHAIR: Order! Mr Shoebridge, you have had your time. That is not a question; it is a commentary. I ask that you be courteous to the witnesses.

The Hon. LYNDA VOLTZ: I am not quite clear how the provisions within the Government Information (Public Access) Act that require that information does not get released into the public domain for public use relate to the bill that is before the Commonwealth, which allows information to be handed over from the State to go into a large database and for the Commonwealth Minister to make a decision to release that information to private organisations. No-one has a problem with national security and no-one has a problem with law enforcement; everyone has—I suspect—a problem with private information being used in this way. If we just take "reasonable use", given that we have State-run insurance schemes, would that be a "reasonable use"? For example, given that the Government identified that fraud within compulsory third party schemes is a huge issue, it could allow the insurance companies access to the scheme. What are the safeguards to the community if that is the decision of the Minister?

Ms TYDD: Speaking within the jurisdiction of an information commission while also recognising the general provisions as I understand them, my colleague commenced referring to some of the safeguards. Another safeguard that may be relevant to your question is the requirement for local government or non-government entities requesting identity-matching services to be covered by the Commonwealth Privacy Act, State legislation or an agreement with the responsible department with equivalent provisions and in that regard maintaining the safety provisions that are operable at a Commonwealth or State level.

The Hon. LYNDA VOLTZ: What in the Commonwealth Privacy Act would prohibit that information being passed to an insurance company?

Ms TYDD: I could not speak to the Commonwealth legislation in relation to privacy. But I do have great confidence in the involvement of the Commonwealth Privacy Commissioner and all privacy commissioners, including my colleague, in consultation.

The Hon. LYNDA VOLTZ: I am not questioning whether you have confidence in them; I am asking where is the protection that means that the information is not handed to an organisation such as an insurance company?

Ms TYDD: I would not feel competent to provide a response that goes to the operation of the Commonwealth privacy legislation.

The Hon. LYNDA VOLTZ: But as a person who is representing the New South Wales Information Commissioner and the Privacy Commissioner, this would be a fundamental question for people in New South Wales about their information, which is now being handed over to the Commonwealth. They would assume that their frontline protection on that information is your office and that there would be safeguards built in.

Ms TYDD: In response to that question I would have regard to the objects of the bill as I understand them to be, in terms of national security and law enforcement, and echo my colleague's comments that the matter remains before the committee.

The Hon. LYNDA VOLTZ: If that is the case would it not make sense to restrict any information handed over to government agencies?

Ms TYDD: Through the Commonwealth scheme?

The Hon. LYNDA VOLTZ: Under the Commonwealth bill. Would it not make sense for the States to say, "We are happy to be part of law enforcement and we are happy to be part of any national security scheme. We think to satisfy everybody's concerns this information should be restricted to government agencies"? Would that not make sense?

Ms TYDD: In terms of the policy intent I think the Commonwealth legislation makes the objects clear. I imagine that there will be other witnesses appearing today who may be better qualified to comment on the Government's position than I would be as an independent statutory officer.

The Hon. LYNDA VOLTZ: But within the legislation it does allow it to be handed to private companies, does it not?

Ms TYDD: It appears that there are a number of other safeguards and checks and balances that might be applied.

The Hon. LYNDA VOLTZ: No, that was not my question.

Ms TYDD: It does appear to countenance consideration of non-government entities requesting identity-matching services to be involved, yes.

The Hon. LYNDA VOLTZ: And in those instances people would want to be assured that written in the legislation were safeguards around what information was provided to private companies.

Ms TYDD: I think the safeguards are the ones that I would currently call out and that my colleague has identified. They go to the "reasonable need" and "specific purpose" provisions and to maintaining coverage by either the Commonwealth Privacy Act, the State legislation or an agreement.

The Hon. LYNDA VOLTZ: Okay, so for "reasonable need", I have given the example of an insurance company as a possible reasonable need or, perhaps, private hospitals.

Ms TYDD: Again, as the bill is before committee, there may be other factors under consideration. It appears to be largely directed to national security and law enforcement purposes.

The Hon. LYNDA VOLTZ: Have you thought about these implications and have you written seeking clarification?

Ms TYDD: Our involvement has been by way of submissions made through the IPC. They have largely been the domain of the Privacy Commissioner and the former Privacy Commissioner.

The Hon. LYNDA VOLTZ: In your submissions have you raised those issues and sought information on the safeguards and, if so, what has been the response?

Ms GAVEL: We have raised a number of issues but, as you are aware, that Commonwealth bill is currently in committee and is under consideration by the committee. I imagine that the committee will have recommendations that they will be making at the end of that process.

The Hon. LYNDA VOLTZ: But the committee is not the safeguard, is it? The safeguard that has been put in there is that the Minister consults with the Privacy Commissioner.

Ms GAVEL: That is a significant safeguard but, as I said earlier, my understanding is that at the moment organisations can only have access through the participation agreements and if private organisations were to be given access—and I understand there is concern about that—it would be on the basis of a "yes" or "no". They would not be receiving personal information. For example, in the case of whether somebody is who they say they are, it would be a "yes" or "no". They will not receive personal information back in response. That has certainly been part of the discussions.

The Hon. LYNDA VOLTZ: But that will not be within the legislation.

Ms GAVEL: It will be within the governance information underpinning the legislation. I am sorry, I know you do not want questions on notice, but—

The Hon. LYNDA VOLTZ: You can take it on notice. I am happy for you to take it on notice, but we would need it pretty quickly.

Ms GAVEL: I can check whether it is in the participation agreement or not.

Mr DAVID SHOEBRIDGE: And any reference to the objects of the bill, given that the Commonwealth bill contains no objects. Ms Tydd gave a number of references to the objects of the Commonwealth bill. I would be interested in that being clarified.

The CHAIR: We will come back to that and will decide that at the end.

The Hon. DAVID CLARKE: I have a question for Ms Falstein. In recommendation 11 of your submission you request a disclosure provision for people applying for or renewing licences. How would you like to see this occur?

Ms FALSTEIN: One of the issues that we have with the New South Wales bill is that sections 9 and 10 of the Privacy and Personal Information Protection Act no longer apply. My reading of that is that you therefore do not have to notify—

The CHAIR: Sorry, just to clarify, did you just say that the Privacy and Personal Information Protection Act will not apply?

Ms FALSTEIN: Yes.

Dr LYNCH: Sections 9 and 10 in the New South Wales bill.

Mr DAVID SHOEBRIDGE: They are the disclosure obligations.

Ms FALSTEIN: That means that you do not have to tell people who have licences that this is what their information is going to be used for. That is my understanding of that exclusion. We feel that you should tell all driver licence holders that this is what their information is going to be used for. We initially suggested that at least new driver licence holders or renewing licence holders should have that information passed on to them so they know what is happening with their photos and driver licence information. But we think that everyone should be advised of what their information is now going to be used for. There has been no consent to this particular use at this stage.

The CHAIR: I have a question for all the witnesses. Is it not a long bow to draw to say that anyone can access this information? That is not the intent of this legislation. The intent is for agencies, for very specific purpose, subject to checks, to access this information in a very limited way for the purpose of criminal investigations, is it not? It is not for insurance companies and others. I understand that in certain circumstances anything might happen with any bill at any time, but that is not what we are talking about here, is it?

Ms TYDD: Chair, I am happy to also address the issue of referencing the objects of the Act as opposed to the purpose, as I understand it, of the Act. Clearly, "purpose" was my desire for outlining the purpose of the Act. As I understand it, law enforcement agencies will be able to use the capability's facial identification service for a limited number of defined purposes, including protective and national security, community safety and law enforcement.

The CHAIR: In limited circumstances, particular agencies will be able to share this information. At the moment, what is the situation? It is not like they cannot share information. My understanding is that they can inquire of each other: "We have this person who may have committed a serious crime". No-one wants to scaremonger but we all remember back to this time a couple of years ago the serious incident in New South Wales. Surely the intent is that we have a faster and efficient way to identify a person in given circumstances; it is not a free for all of information, as is perhaps being proposed. Would you care to comment on that?

Ms GAVEL: My understanding is that that is correct. Although the Commonwealth has a document verification system that is a similar system, of course, being paper based, it is not as fast as this will be.

The CHAIR: How is it exercised at the moment?

Ms GAVEL: I understand that documents can be checked with the Commonwealth through their document verification system. I am not highly up on the details of that but I imagine that the Home Affairs people, who are coming later, will have more insight.

The CHAIR: It is an email, is it not? Literally one agency sends an email to another one and says "Can you verify this?"

Ms GAVEL: Yes, it is.

The CHAIR: This is quite serious stuff we are talking about. In a serious situation, a criminal act, the intent clearly is to have fast information sharing, if necessary, to protect citizens.

Ms GAVEL: That is right, and recognising that because this system will be faster and because it is sharing very sensitive biometric information, which is highly personal information, there need to be more stringent privacy and security measures in place than are actually applied to the Document Verification Service [DVS], which has quite stringent ones, as I understand, already. That is part of the role that I have had in consulting with the Commonwealth on that and that all State and Commonwealth privacy commissioners have had.

The CHAIR: Can you tell us and expand on that consultation process?

Ms GAVEL: It has gone on over a number of years and we did document some of the processes that the Information and Privacy Commission [IPC] has been involved in, in our submission. The most recent one that I was involved in was in about March this year, a roundtable of privacy commissioners with the Department of

Home Affairs to look more closely at some of the compliance documentation that underpins the scheme and also to have input into the latest privacy impact assessment that has been done. There have already been two done, as I understand it.

The CHAIR: There have been two lots of consultation?

Ms GAVEL: Two different privacy impact assessments. The first one I think was done on the identity hub, the second one on the—one of the aspects of the facial matching aspects of the scheme and the current one is looking at the design operating model and governance arrangements of the scheme.

The CHAIR: The information we are talking about essentially is a photo, date of birth, gender and an address. Is that correct?

Ms GAVEL: That is right.

The CHAIR: Is there any more than that?

Mr DAVID SHOEBRIDGE: You have biometrics.

Ms FALSTEIN: There is actually more.

Dr LYNCH: There is biometrics but there is a huge list, a huge definition—it is a page-and-a-half long—of what "information" means in the Commonwealth Act and it excludes—

The CHAIR: But not in this bill?

Dr LYNCH: In the Commonwealth bill.

Ms FALSTEIN: Actually, in this bill there is something that is a bit concerning, I think, because when they talk about "information" in—

The CHAIR: It is not religious persuasion, it is not any of those other things. It is this person who this photo represents. It is identity matching, is it not?

Ms FALSTEIN: "Associated information" is in the definition. It says it includes—

The CHAIR: I have the bill. I understand what the bill says.

Ms FALSTEIN: But it "includes", it is not "this is it". I am just wondering what "includes" means? Does that suggest that something else might be included, or what is not included?

The CHAIR: When we talk about handing over information to a private organisation, my understanding is that we cannot just hand over information without robust checks. It will not be a publicly available entity. It is limited to specific government agencies. Is that not correct?

Ms GAVEL: The Commonwealth Government, as I understand it—and again, I think this would be better directed to Home Affairs—but my understanding is that there has been some discussion around whether banks or those sort of entities that need to conduct identity checks would be able to check through the system for a "yes" or "no" response on whether the person is who they say they are.

The Hon. SCOTT FARLOW: So if somebody presents to a bank giving an identity document to access an account, for instance, they could run a check on that and be told "yes" or "no"; not access the information.

Ms GAVEL: Yes, that is right; that is my understanding. Again, I would emphasise that you will have the Department of Home Affairs officers here who will be able to answer in more detail those aspects.

The Hon. DAVID CLARKE: Would you agree with that, Ms Falstein?

Ms FALSTEIN: There are a number of organisations that will be able to access the information either through the Commonwealth bill or even in relation to the New South Wales bill, as I see it, because the New South Wales bill permits access by an authorised government agency, and that includes the authority and/or any agent of the authority. My understanding is that agents of the authority are wide and numerous and do all sorts of things and they do not necessarily relate to law enforcement objects.

The CHAIR: Are you aware of particular personal information being collected by roads agencies that you are concerned about being shared with law enforcement agencies?

Ms FALSTEIN: No, I am not concerned about law enforcement sharing. But, for example, Roads and Traffic might be sharing information with other agencies because they are also collecting information of this Interoperability Hub. It works both ways—you are putting information in but you are also collecting information, which will be shared.

The CHAIR: With law enforcement?

Ms FALSTEIN: Not necessarily with law enforcement, with any authorised government agency or with any agent of the authority.

Mr DAVID SHOEBRIDGE: Or a service prescribed by the rules.

The CHAIR: Sorry, I am asking the witness. Your submission talks about this close to real-time mass surveillance, I think it said. I am just wondering what information you base that assessment on.

Dr LYNCH: First of all, the Prime Minister took a commonsense view of this when it was first announced, as you would if you read through it. You might recall he made a statement saying, "This will enable us to"—I do not have his exact words in front of me but he was really saying "This will enable, for example, us to be able to identify anyone"—I think he said—"going into a football stadium or into a big concert". It was words to those effect, and he obviously got another briefing on this and came out later and said, "I know this will not be possible because"—if we are going to call it "capability"—"the capability will not be storing images captured by closed-circuit television". That is true, but that is not the point.

As I keep saying, the thing that makes this radically speedier and different from anything we have had before is the enhanced capacity for a photograph, an image of someone who is unidentified, or numbers of people, to be very quickly, almost real-time, identified. Once you have identified them through the Face Identification Service [FIS], you would have access to a whole lot of other information. We are relaxed around that kind of context—"we" being Civil Liberties—if what we are talking about is a situation, a terror event, anything that seriously threatens public safety. We are not relaxed about that if it gets extended to either intelligence agency or someone in the Police Force wanting to know who is attending certain demonstrations, who is—

The CHAIR: I think the threshold is to investigate offences with no less than three years imprisonment, so we are not talking about minor offences.

Dr LYNCH: No, I am talking about—

The CHAIR: The information being shared?

Dr LYNCH: —information sharing, and presumably, if it is a law enforcement or an intelligence agency seeking it, they will be seeking it theoretically or in relation to some potential criminal activity. Of course that is that other whole aspect we just mentioned in passing. I have recently seen a quite terrifying documentary done—again I would have to send you the details. I think it was a Swedish doco looking at predictions being done through this kind of stuff in terms of who was going to commit crimes, who is dangerous in Manchester and somewhere in Canada. The police were very proud of this, but it was a very, very frightening kind of thing.

The CHAIR: Siege situations are frightening.

Dr LYNCH: Can I just say I think there is also another confusion running that might be at cross-purposes. There are different levels and non-government and local government do not have access to the FIS. They do to the Face Verification Service [FVS]. We would argue it is better for non-government not to have access to either of them. We would argue that, at the moment, the criteria determining local government access does enable them to come in on almost anything. If we are going to let local government in, it should be a much tighter set of provisions. We are never comfortable with that being left to ministerial discretion to come up with a set of rules or government agreements.

The CHAIR: Thank you.

Mr DAVID SHOEBRIDGE: My question is to both Ms Gavel and Ms Tydd. In your submission and in your oral presentation you talk about there being a legitimate public purpose because this is about law enforcement and national security, among other purposes. But at no point have you addressed the very broad definition "additional purpose"—one of a number—which is community safety activities which have an inclusive definition, which begins:

> This subsection covers promoting community safety, including by identifying …

Are you not at all troubled by the fact that all of this deeply personal information can be shared for a purpose as amorphous as promoting community safety? What do you understand to be the boundaries of that?

Ms GAVEL: Can I just check, is that from the Commonwealth bill or the State bill?

Mr DAVID SHOEBRIDGE: From the Commonwealth bill, section 6 (6).

Ms TYDD: I think the submission that we have jointly provided and our evidence today really does highlight that we are acutely aware of the safeguards. We recognise the need for safeguards in the Government

Information (Public Access) Act as you would see as exemptions and safeguards that apply in relation to privacy. We also recognise the complexity of the scheme, particularly as would be characterised as a two-layered approach. We heard from witnesses that local government might have access to the identity verification. One of the additional safeguards that, in my understanding, is apparent or should be operable is restricting local government and non-government access in circumstances where identity verification is reasonably necessary and is done with the consent of the individual involved. I think that our concerns remain in relation to appropriate safeguards and they are expressed in our submission. They go to the particular aspect of the scheme that is being operationalised and, of course, to those purposes that I referred to earlier. They may have an effect that is applied differently to those stages and to the entities that might be involved.

The CHAIR: Thank you very much. I am sorry it has been brief today. We have to finish there. I thank all the witnesses for attending and providing written submissions so quickly. One question was taken on notice. Ms Gavel, can you provide that to the Committee secretariat by tomorrow morning?

Ms GAVEL: Yes. Thank you.

The CHAIR: Thank you.

(The witnesses withdrew)

PATRICK SEEDSMAN, Senior Legal Counsel, Roads and Maritime Services, affirmed and examined

JUSTIN GRIFFITH, Director IT, Strategy and Architecture, Roads and Maritime Services, affirmed and examined

MARK JENKINS, Assistant Commissioner, NSW Police Force, sworn and examined

ANDREW RICE, Acting First Assistant Secretary, Identity and Biometrics Division, Department of Home Affairs, sworn and examined

STEVE WEBBER, Assistant Secretary, National Security and Law Enforcement Branch, Legal, Department of Home Affairs, affirmed and examined

The CHAIR: I remind all witnesses that mobile phones should be turned to silent for the duration of the hearing. I welcome our witnesses. Did any of you have an opening statement? I ask that they are brief, given the limited time we have today.

Mr SEEDSMAN: I have a short opening statement.

The CHAIR: Thank you. Is it just the one?

Mr RICE: I have one too.

The CHAIR: Thank you.

Mr SEEDSMAN: Part 3.5 of the Road Transport Act 2013 limits disclosure of driver licence photographs as follows: to New South Wales police; to interstate driver licence agencies, for road transport law criminal proceedings; to the Sheriff to recover fines; and as otherwise permitted by law including by regulation. The bill seeks to amend part 3.5 to permit Roads and Maritime Services [RMS] to upload driver licence images to the Capability. While RMS participation will initially be limited to uploading images to the Capability, there is scope in future for RMS to choose to also become a user of the Capability via the one person, one licence service known as OPOLS.

RMS has used its own facial recognition system for many years to detect fraud but RMS' system is limited to comparing a customer's image against RMS' own photo database. OPOLS, however, would permit RMS to check an image against driver licence images of other road agencies too and so OPOLS would allow RMS to prevent fraud by checking whether a customer holds a driver licence in another jurisdiction under another name. Should RMS choose to use OPOLS then it is conceivable that it could be used at the point in time when the customer attends a service centre to have their photo taken for their licence. Since RMS has delegated its customer service functions to Service NSW the bill defines RMS to include its agents acting on RMS's behalf.

Section 9 of the Privacy and Personal Information Protection Act, commonly known as PPIPA, requires RMS to collect personal information directly from the customer. If RMS chooses to use OPOLS then matched images will be downloaded from the hub rather than collected directly from the customer, hence the bill provides an exemption from section 9 of the Privacy and Personal Information Protection Act. RMS' existing privacy statement already informs customers that RMS may use and disclose their personal information in order to verify their information.

Obviously it is not possible to retrospectively update privacy statements to refer to the Capability, hence the bill proposes to exempt RMS from the obligation in section 10 of the Privacy and Personal Information Protection Act to provide a privacy statement. Nevertheless, RMS proposes to progressively update all of its privacy statements in 2019 so that they explain RMS's participation in the capability to customers. RMS will be consulting the New South Wales Privacy Commissioner on the refresh of its privacy statements.

Mr RICE: Thank you for the opportunity to appear before the Committee today. In 2007 the Council of Australian Governments agreed to the National Identity Security Strategy to help strengthen collaboration between the Commonwealth and the States on efforts to combat identity crime. Since then the cause of identity security has advanced substantially, not least due to the shared initiatives such as the Document Verification Service [DVS] and the development of several national standards related to identity management. Identity crime causes substantial harm to the economy and individuals each year and is a key enabler of terrorism and serious and organised crime.

The forthcoming "Identity Crime and Misuse in Australia" report from the Australian Institute of Criminology indicates that identity crime impacts on around one in four Australians throughout their lifetime, with an estimated annual cost of $2 million. We also know that due to the growing sophistication of criminal

syndicates and the technologies now able to support them, fraudulent identity credentials are difficult to distinguish from the genuine article, and name-based checking tools such as DVS cannot detect when a fraudulent photo is combined with otherwise legitimate details. That is why back in 2014 we began the journey with facial biometrics conceiving the National Facial Biometric Matching Capability and the Face Matching Services that put it into practice.

After a sustained period of collaboration with the States and Territories, we reached an Intergovernmental Agreement on Identity Matching Services in October 2017. We are now in the process of delivering a suite of face-matching services to complement the DVS and to help further combat the pervasive problem of identity crime affecting many Australians. Of course we also expect the identity matching services implemented through the intergovernmental agreement will assist with a range of national security, law enforcement and community safety activities and will help to improve road safety through, for example, the detection of people using multiple fraudulent driver licences.

For our part the Commonwealth has introduced the Identity Matching Services Bill 2018 to Parliament to strengthen the legal basis for the Department of Home Affairs to collect, use and disclose identification information in order to operate the services. As described in our submission, the bill has a range of privacy, accountability and transparency measures to ensure appropriate safeguards exist in relation to the proper handling of identification information. The Department of Home Affairs welcomes the introduction of the New South Wales legislation to support the State's participation in the national facial biometric matching capability.

Mr DAVID SHOEBRIDGE: Mr Seedsman or Mr Griffith, you would have heard the evidence from the privacy and information commissioners. When we asked them what the final shape of the privacy protections would be federally they said they could not really answer because the bill was still in committee federally. Do you agree with their evidence?

Mr SEEDSMAN: I think they also make the point that there is a whole suite of governance documents that will apply, and that it is the case that in addition to the top level documents, participation agreement and hosting agreement and the intergovernmental agreement, there is a whole suite of other documents which give each agency, including RMS, ultimate say over who accesses its data.

Mr DAVID SHOEBRIDGE: But in the legislative protections we are looking at, State and Federal, do you agree with their evidence? We do not know what the shape of the final legislative protections federally will be because the bill is still in committee?

Mr SEEDSMAN: That is certainly true. But RMS is taking comfort from the fact that primarily access is for law enforcement. Any other access would require RMS approval which would require customer consent.

Mr DAVID SHOEBRIDGE: That is in the bill but we have not seen what the final shape of the law looks like.

Mr SEEDSMAN: That is true.

Mr DAVID SHOEBRIDGE: Why are we rushing this bill through New South Wales to hand over information to a Federal scheme that has not been legislated for? What has been the rush to get it through in the last six days of this Parliament?

Mr SEEDSMAN: I am sorry, I cannot comment on that. I am involved in the drafting of legislation but as to the timetabling—

Mr DAVID SHOEBRIDGE: Is there any agency imperative to have this legislation adopted by the end of this year before the Commonwealth legislation has been adopted? Is an imperative being driven by your agency?

Mr SEEDSMAN: I believe the timetable for RMS is to upload images in August next year. I would hazard a guess that perhaps with the State election in March there might be some concern that Parliament might not meet again until April or May and that might not leave much time for the State legislation.

Mr DAVID SHOEBRIDGE: Are you guessing at this or is that what you understand?

Mr SEEDSMAN: I am not the subject matter expert on that issue.

Mr DAVID SHOEBRIDGE: I refer to the protections about disclosure. Section 16 onwards of the Federal bill provides for the legal authority for the information to be disclosed by the Commonwealth entities. That would be a sufficient legal basis to disclose what was previously State information in State driver licences, would it not? You do not need a separate sign off by the State agency before what was previously New South Wales information is shared through the hub?

Mr SEEDSMAN: No, that is actually correct. Each agency has ultimate control over what other agency accesses its data in the hub.

Mr DAVID SHOEBRIDGE: What are the legislative restrictions under this bill that limit the sharing of information once it is provided?

Mr SEEDSMAN: Under the New South Wales bill?

Mr DAVID SHOEBRIDGE: Under the New South Wales bill.

Mr SEEDSMAN: The governance documents in the scheme. So applications need to be made on each occasion to the agency who holds the data, explaining the legislative basis for the access and providing sufficient governance assurance to, in this case, RMS.

Mr DAVID SHOEBRIDGE: The bill that is before the New South Wales Parliament just simply hands over the information to the capability, if we could describe it that way, and the only restrictions are upon New South Wales agencies as to how they keep information either that they have provided to or received from the capability? The New South Wales bill puts no limits on the Commonwealth.

Mr SEEDSMAN: That is true. The limits are in the in the governance documents.

Mr DAVID SHOEBRIDGE: The Federal bill says:

> For the purposes of State and Territory laws that limit disclosure of identification information by an authority of a State or Territory but have an exception for disclosure authorised by a Commonwealth law, this Part [being part 3] authorises such disclosure …

So once the information is handed over there is a legislative authority of disclosure under the Commonwealth bill, is there not?

Mr SEEDSMAN: I am not an expert on Commonwealth legislation so I cannot really comment on that.

Mr DAVID SHOEBRIDGE: For what purposes will your agency be using the information obtained from the capability?

Mr SEEDSMAN: It is my understanding that RMS does not have any present proposal to use information from the capability.

Mr DAVID SHOEBRIDGE: So the evidence the Committee has received from others about testing for multiple driver licences and fraudulent driver licences is not currently your intention?

Mr GRIFFITH: The One Person One Licence Service in issuing a licence would allow us to do a check into the system to determine if there is any fraudulent activity. So we would use the database for that check under that service.

Mr DAVID SHOEBRIDGE: I thought Mr Seedsman said there was no current intention to use the database? I do not understand, your evidence seems to be contrary?

Mr GRIFFITH: No. I think Mr Seedsman covered it in his covering note. The initial rollout of the service is merely for New South Wales to provide the data to the capability. There is the One Licence One Person Scheme, which is not yet defined, and we have not decided whether we will take that service up and what we will do as part of it.

Mr DAVID SHOEBRIDGE: So with no current plans for your agency to access or use the capability, there is no reason to rush this legislation through, is there? You have no actual plans to use this?

Mr GRIFFITH: Correct.

Mr DAVID SHOEBRIDGE: Mr Rice, what do you understand to be the bounds of community safety activities or actions that promote community safety as defined in the Commonwealth bill—section 6 (6)?

Mr RICE: As it is in the bill. One thing I would point out, having heard the evidence of the previous witnesses—

Mr DAVID SHOEBRIDGE: I saw you, and I think that has been beneficial.

Mr RICE: One thing I would point out is that our bill makes provision for community safety measures to be applicable where there is a concern about a person being harmed or a person doing harm. In that kind of sense those are the controls we would see around the use of the capability in a community safety sense. Beyond that—and maybe this is something that Assistant Commissioner Jenkins can talk about—we are just providing a tool that can be used by law enforcement but with a range of controls on it.

Mr DAVID SHOEBRIDGE: If it was limited to preventing physical harm or reporting missing persons, the legislation would have been drafted in that way. But the legislation is drafted as promoting community safety, including by doing that matter. So you have got an inclusive definition; it is not limited by the categories of information you are identifying. From a Commonwealth perspective for what other things will the information be used to promote community safety?

Mr RICE: Are you asking about the kinds of events? Is that what you mean?

Mr DAVID SHOEBRIDGE: For what other purposes will the information be used insofar as it promotes community safety?

Mr RICE: The service is there principally—and this is really the identification service but the Face Verification Service is potentially applicable there—to verify identity and to identify unknown persons who may be a risk of harm or of creating harm.

Mr DAVID SHOEBRIDGE: People who may not have committed an offence to date but might be future troublemakers? Identifying them would be promoting community safety?

Mr RICE: One of the things about the Commonwealth Bill, which is really important to say, is that it does not give the power to any agency to use the capability; it gives the Department of Home Affairs the ability to collect, use and disclose the information. A party that is using the service needs to have a lawful basis in order to use the service and it will be, I guess, nine jurisdictions will have a range of different laws in place that will allow them to use the capability in the context of community safety to identify persons in the way I described earlier on.

Mr DAVID SHOEBRIDGE: So if there is a Victorian police outfit that is looking at potential future crime, and that was lawful in Victoria, they could access it for that purpose?

Mr RICE: They can only access it if they meet the requirements of the Act in terms of—

Mr DAVID SHOEBRIDGE: Promoting community safety?

Mr RICE: Yes, and having a lawful purpose themselves.

Mr DAVID SHOEBRIDGE: It ticks the box.

Mr RICE: So if there is something on the statute book that allows them to do that, potentially.

Mr DAVID SHOEBRIDGE: The protection that is contained in section 7 (3) (b) of the Commonwealth bill about handing over facial verification information to local government and non-government entities, includes the individual has given consent, is that right?

Mr RICE: That is right.

Mr DAVID SHOEBRIDGE: Does that include consent that is contained in those finely typed eight-, nine-, 12-, 30-, 40-paragraph-long consent provisions that you click okay to when you are accessing either a telecommunication service or the New South Wales Opal Card or whatever?

Mr RICE: I think Mr Seedsman has addressed some of that, but if I can just back up for a moment. We have talked a bit about the Document Verification Service—

Mr DAVID SHOEBRIDGE: Perhaps if you could just answer the question I put to you.

Mr RICE: Like I said, Mr Seedsman has talked about the privacy policy work and the disclosure to users that will be put into place.

Mr DAVID SHOEBRIDGE: Mr Rice, I am asking you about consent so that information can be given to private businesses and entities.

Mr RICE: And I am answering in that respect. I was also going to make the point that we have been through this with the Document Verification Service over a period of—I think private sector users have been using it for four years now. So we have been what consent means and how it is captured in an appropriate way through with a range of Commonwealth and State agencies. What we intend to do is in effect put in place the same provisions, updated as necessary, in order to govern the operation of the Face Verification Service.

The Hon. LYNDA VOLTZ: No-one has a problem with using this for law enforcement and national security. Why not just restrict this to government agencies?

Mr RICE: Is that question addressed to me?

The Hon. LYNDA VOLTZ: Yes.

Mr RICE: At the end of the day the governments of Australia have determined that they have an interest in providing it for a wider set of uses. You might have seen in our submission that we provided, that we talked about some of what I would call high-end identity crime methodologies that are being employed at the moment—once again, Assistant Commissioner Jenkins can probably chime in here. We provided the Document Verification Service back in 2014 to the private sector and one would have thought that identify crime would have gone away, but it was pretty clear from Australian Federal Police and New South Wales police operations that quite early on criminals had worked out how to overcome the fact that if all you need is the credential information—name and date of birth—you can get that by a variety of means and if you put another face on that then that document, when presented, will pass. We believe, and I think the governments of Australia believe, that identity crime should be addressed as holistically as possible. It is not just a government role; it is potentially private sector. As I said at the beginning in my opening statement, identity crime costs a considerable amount of money every year and a lot of that impact is on the private sector as well.

The Hon. LYNDA VOLTZ: If you want to address identity fraud, for example, in the banking sector, if they are not getting access to the biometrics anyway—it is only if someone has a suspicion that someone who has come in may be an identify fraud—why is the Australian Transaction Reports and Analysis Centre (AUSTRAC) not the appropriate place to hold that biometric data and do the check?

Mr RICE: We have had some preliminary discussions with the banks about how they might use the Face Verification Service and they would see it as supporting their obligations under Commonwealth legislation, the Anti-Money Laundering and Counter-Terrorism Financing Act, which goes to knowing your customer. In many cases that will be for initial account enrolment, not necessarily just in a fraud sense.

The Hon. LYNDA VOLTZ: Sorry, you are going very quickly. Can you just explain why if they do not have access to the data and they have to apply for it anyway—

Mr RICE: The way it works at the moment is, if I went into a branch or, indeed, as you are increasingly seeing globally, smartphone enabled applications for enrolment, then there is a capturing of personal information and there is capturing of an image in that process. The banks will have decided for their own risk management purposes, and in some cases because of their obligations under legislation, that they want to verify that information. We are giving the ability to add a face to what they already have with the Document Verification Service. So they will collect that information and they will then be able to query our system. As the previous witnesses said, all they will get back is a yes or no answer, which is all they get under the Document Verification Service at this time.

The Hon. LYNDA VOLTZ: They capture a photo?

Mr RICE: Not at the moment. For the reasons I described earlier about where criminal methodologies are going we would be advising them, and our knowledge of global developments in the banking sector would suggest, that that is the way they are moving, that they will be looking to capture an image in the first instance. To the point that was raised earlier, they are capturing that image. They are then providing that to be matched against the system, and all they receive back is a yes or no. So they already have to have a basis to collect.

Mr DAVID SHOEBRIDGE: Is that image added to the database, the capability?

Mr RICE: No.

The Hon. LYNDA VOLTZ: My point is that they are not actually accessing the system. They are asking someone else to access the system to check an identity?

Mr RICE: No. If they are given permission—once again going back to what happens with the Document Verification Service—they are authorised, contracted users to our service. They have a connection, in some cases directly and in other cases through an agent, that allows them to query the system.

The Hon. LYNDA VOLTZ: Who would that agent be?

Mr RICE: In current terms in the Document Verification Service, it is a range of commercial providers. You probably know of some of them. VIX Verify is one and Experian is another one, I think.

The Hon. LYNDA VOLTZ: You will be giving commercial operators access to the system?

Mr RICE: If it is agreed by the governments of Australia that that occurs, yes. And if you consult the intergovernmental agreement [IGA] you will see that there is a supplementary ministerial decision that would have to be taken about access to the private sector.

The Hon. LYNDA VOLTZ: Have any of the States expressed concern about that?

Mr RICE: The IGA has been signed by all of them and the only jurisdiction that put qualifications on their provision of data was the Australian Capital Territory [ACT].

The Hon. LYNDA VOLTZ: Have any other States expressed recent concern regarding privacy?

Mr DAVID SHOEBRIDGE: Like Victoria.

Mr RICE: You may be aware that the Victorian Government provided a submission to the Parliamentary Joint Committee on Intelligence and Security, where they raised some concerns about our bill allowing for private sector access. We responded in committee to the effect that our bill was about futureproofing. At the end of the day it is still a decision for all the governments of Australia as to whether the private sector gets access to driver licences.

The Hon. LYNDA VOLTZ: What are you going to do when the information provided from the State does not marry up with the information held by the Commonwealth? You have a person on your system and the information provided from the State on that person is different.

Mr RICE: At the end of the day there is not one database, I would like to make clear. That is something we cannot seem to crack through on publicly, I suppose. There is a passports image database, there is a visa and citizenship holding in our own department, and we will be creating the driver licence image. They will be separate databases in the system that can all be queried. It is not a question of the driver licence images updating the passports database. The integrity of the databases is maintained at the credential level, so passports maintains theirs, driver licence—

The Hon. LYNDA VOLTZ: I understand that. Say my passport has a different name and date of birth to my driver licence?

Mr RICE: That will come out. If the system is used by an authorised user, then we are in the territory of fraud potentially, fraud investigation.

The Hon. LYNDA VOLTZ: My driver licence is different to my passport because I had a driver licence a long time before I had a birth certificate. What happens in the system when the State information is going to be different to the federally held information?

Mr RICE: You are taking us into other territory, which is in the area of identity-proofing guidelines, which has been an area of endeavour between all the governments of Australia. We continue to work on best practice approaches to managing information in these various credential databases. It is a long journey.

The Hon. DAVID CLARKE: Mr Seedsman, can New South Wales withdraw from the capability if another State was not able to meet our privacy requirements?

Mr SEEDSMAN: Yes.

The Hon. DAVID CLARKE: What is the error rate for this technology?

Mr SEEDSMAN: I think that is a question for Home Affairs.

Mr RICE: Biometrics is a probabilistic process. The error rate depends on the matching threshold that is put in place, and that is directly related to the risk tolerance of the users. The answer from significant international bodies that look at the quality of matching, the United States Government has a National Institute of Standards and Technology that does a lot of testing. Their advice is that accuracy is improving steadily. A lot of things influence quality as well. In the case of matching a driver licence image which has been taken in a controlled environment—very good chance of success. When you are talking about closed-circuit television type images—not quite so good.

The Hon. DAVID CLARKE: Has the technology been trialled in Australia?

Mr RICE: As my colleagues have said, facial recognition has been used in RMS for some time. We use it in the Department of Home Affairs. You do not get a passport issued without some form of face matching going on in the Department of Foreign Affairs and Trade. So it has been used.

The Hon. DAVID CLARKE: What reporting and audit systems are in place for the scheme?

Mr RICE: The intergovernmental agreement, the Commonwealth bill and the governance agreements that have been described today, all provide a requirement for audits to be done on the use of the system by users, independent audits to be done. We also have an arrangement, we have a memorandum of understanding with the Office of the Australian Information Commissioner to do annual audits on our system as well.

The Hon. SCOTT FARLOW: We have heard a lot today from people who have said they would be happy if access was restricted to law enforcement agencies. Could you go through some of the government agencies that will be able to access this information? What are we looking at? I think the New South Wales legislation has authorised an agent. What does that mean? What does that pick up?

Mr RICE: Just to give you a sense of some of the agencies that are considering using it, I will break it up into two bits. The face identification service is prescribed in legislation. It is listed police, security, and anti-corruption agencies in the Commonwealth and the States. There is no-one else who is going to get access to the system, other than those prescribed.

The Hon. SCOTT FARLOW: When it comes to facial identification, that is the list?

Mr RICE: That is the list, yes, and you will find it in our legislation. In the case of the Face Verification Service, the interest that we have had in using it from a range of Commonwealth and State agencies, I would put them broadly in the categories of, obviously the road agencies, also regulatory agencies, some of the large Commonwealth agencies, the Australian Taxation Office, the Department of Human Services, in part for fraud investigation, but also for citizen access and fraud management at that channel. There is also a significant piece of work you may have seen announced by the Federal Minister for Human Services and Digital Transformation about a week ago, about the Digital Transformation Agency and the development of a digital identification. The use of the Face Verification Service is fundamental to that. I think if we followed where the Document Verification Service has gone we will see, broadly speaking, law enforcement and regulatory service delivery agencies looking to use it.

The Hon. SCOTT FARLOW: The Chair outlined to our previous witnesses what currently happens. It was put to those witnesses, and correct me if I am wrong, that the current system of getting a check like this is sending an email with an attached photo and waiting for verification. That seems like a relatively unreliable process to me.

The CHAIR: And slow.

The Hon. SCOTT FARLOW: And slow, and potentially there could be the case where somebody will not pick up on an email. How does it work? Is that how it works?

Mr DAVID SHOEBRIDGE: I doubt Mr Rice will say it is unreliable.

Mr RICE: What I was going to say is it is not accountable, when there are emails flying around. What we do with this system is put more accountability into the movement of that information. What currently happens with the Document Verification Service is that there is a central router, if you like. Users have an ability to launch a query. If they want to verify my ACT driver licence, then they provide full name, date of birth and credential number, and that is provided through the service to a body which brings together all the national driver licences, and then the answer comes back. It is a sub-second process. We would see something similar occurring with this; it is the same architecture. I have got some diagrams here. If it helps at all, I can hand them out.

The CHAIR: Yes, thank you, that would be helpful.

The Hon. SCOTT FARLOW: Mr Rice, we have heard evidence that some people or agencies or organisations will be able to access it on a yes/no basis. How does that work?

Mr RICE: Essentially, in the case of the document verification service, those three core elements—the credential number, full name and date of birth—are compared against the record in the holding agency and then it is just a system response that says yes/no. It will be the same in this instance. We talked a little bit in the earlier session about what identity information is collected. It is credential information, particularly with the face verification service; we want to as quickly as we can get to the record in question and then the face is presented and what the facial recognition algorithms do is say yes, that is a match to a certain threshold, and provides the yes/no answer back. So it is just a system response.

The CHAIR: Forgive me if this has been asked, is this technology being trialled or is there a proposal to trial it?

Mr RICE: Facial recognition has been in operation for quite some time. If you travel back from overseas and you go to SmartGate, that is facial recognition in operation. It is obviously being used in Roads and Maritime Services. Our knowledge of overseas experiences would suggest that it is used in a range of places as well. It has certainly been around for some time.

The Hon. DAVID CLARKE: There was a report in the *Sun-Herald* on 4 November that indicated that the ACT and Victoria have objected to The Capability. Have they indicated that they have withdrawn from the intergovernmental agency signed at COAG?

Mr RICE: Yes, I saw that report and I am not sure of the providence of the comment about the ACT having an issue. I said before that they prescribed their participation at the time of the signing of the intergovernmental agreement, and the prescription was essentially that they would only permit access to ACT driver licences for the face identification service for counterterrorism purposes.

The Hon. DAVID CLARKE: That was ACT?

Mr RICE: That was ACT. There were no restrictions on Victorian participation. Without knowing what the paper is referring to, I think they are referring in the case of Victoria to the submission to the Parliamentary Joint Committee on Intelligence and Security from a Victorian Minister, and I did mention that earlier on; they had issues around private sector access. It was about issues of the scope of the bill as it related to private sector access and also about the credential images that could be captured.

The Hon. DAVID CLARKE: But that does not mean that they have withdrawn from the intergovernmental agreement at all.

Mr RICE: No. I cannot speak for Ministers but we have had a number of discussions with senior Premier's department officials who have been at pains to say they are still with us and, indeed, are very close to being brought into our technical program for integration of their images.

The Hon. DAVID CLARKE: So that means the report in the *Sun-Herald*, from the information you have, is not correct.

Mr RICE: I do not believe it is correct.

The CHAIR: Mr Rice, did you want to speak to these documents?

Mr RICE: I was just going to say that the Document Verification Service one I handed out, if you look down the right-hand side—

Mr DAVID SHOEBRIDGE: It is not by email.

Mr RICE: No, it is certainly not. The best way to describe it is there is a big router in the middle and on the right-hand side of the page we have got the credentials that are verified there. In the instance of driver licences, we go to a database managed by Austroads, but the other credentials are directly connected. You can see on the left-hand side of the page that there is a range of ways of connecting. We have some users that connect directly to the big router, to the hub, others come through those agents that I was talking about earlier on. That system has been in operation for 10 years; it has been going at a high rate of knots since 2012. The last financial year it did 33 million transactions at an average speed of under one second per transaction and has about 800 private sector users and close to 100 government users. So it has been a big success.

The other diagram I provided to you is the one of the face matching services. I think the important thing to emphasise there is you will see a similar architecture to what we have for the Document Verification Service. Many lessons were learnt in the development of the Document Verification Service around privacy, and they were about not bringing things into central databases. So, once again, you see that big router, the hub, that routs the messages out to, in the case of the passports database and the Home Affairs databases, existing data holdings with facial recognition capability on them. In the instance of driver licences, only two jurisdictions had a facial recognition capability.

We wanted to bring these driver licences together for a range of preventing identity crime and detecting broader criminal and terrorist incidents. For a range of performance reasons it did not make sense, and it certainly did not make sense from a cost perspective, to give every jurisdiction a facial recognition system; so if there is a database, it is that driver licence one, but the driver licence database is segmented by jurisdiction and each segment in the case of New South Wales is controlled by New South Wales authorities. As previous witnesses have said, it is the data holding agencies that grant access to their images, and that is bound up in the intergovernmental agreement.

The CHAIR: So each State controls its own information?

Mr RICE: It does. We are just the host—in fact, the Commonwealth cannot use it in any kind of special way; it can only use it in the way that all other users can if it comes in through the interoperability hub.

Mr DAVID SHOEBRIDGE: You said before it is not one single database; it is a series of databases that are interrogated by the interoperability hub.

Mr RICE: That is right. It is important to say, a series of existing collections.

Mr DAVID SHOEBRIDGE: But the power of it comes by the hub interrogating the various databases and comparing the information it gets from the various databases; that is the new value that is added.

Mr RICE: And also, adding to that, the speed in which it can be done, because it is very slow at the moment and not accountable for the reasons I said before.

Mr DAVID SHOEBRIDGE: I know you cavil with the argument about it being a single database, but the end effect is, because of the interoperability hub, it is as though there were various segments of the one database, it is almost instantaneously interrogated and compared and then the information about one individual is, if you like, brought to the apex in the hub and then provided to whoever asks for the information.

Mr RICE: That is essentially it, yes.

Mr DAVID SHOEBRIDGE: Services that can use the interoperability hub include services prescribed by the rules. Is that right?

Mr RICE: Services prescribed by the purposes in the Act. The rules in our Act are only about changes to the system.

Mr DAVID SHOEBRIDGE: Say, for example, an identity matching service, which is one of the key services identifying if Mr Rice is really Mr Rice, those identity matching services are identified, I think, in clause 7 of the Commonwealth bill. Is that right?

Mr RICE: I think they might be in another part, but it talks about—

Mr DAVID SHOEBRIDGE: The one I have is Face Identification Service [FIS] and Facial Recognition Analysis Utility Service [FRAUS]—

Mr RICE: That is right, the individual services.

Mr DAVID SHOEBRIDGE: —or a service prescribed by the rules.

Mr RICE: Yes. We have talked a bit about face verification and face identification. Mr Seedsman and Mr Griffith touched on a couple of the services that we are providing specifically for road agencies; one of them is a one-to-one service, a verification service, and it was one of the points I made before about the integrity of the data—it gives the agencies a chance to better manage duplicate records. And, as we talked about before, the one person, one licence service is there to allow for better integrity around the issuance of credentials. I think my colleagues here can tell you that there is quite a sizeable amount of interstate licence applications in RMS that comes in any given year, and this would give RMS the opportunity to check against other driver licence agencies.

Mr DAVID SHOEBRIDGE: The legislation you say futureproofs by allowing for private entities to set up an identity matching service.

Mr RICE: No. What it allows for is for those private sector users to use the service in the same way they use the document verification service. They are not a separate service per se they are a user as long as they have a lawful purpose to use it.

Mr DAVID SHOEBRIDGE: Can there be private identity matching services established under clause 7 (1) (f) of the Commonwealth bill? It says "a service prescribed by the rulings".

Mr RICE: In theory if we do see a use for it. We are looking to leverage existing ubiquitous collections: driver licences, 80 per cent of Australians over the age of 16 and 55 per cent of Australians with passports. I am struggling to think of a private sector holding that would be as wideranging. We have no plans for that.

Mr DAVID SHOEBRIDGE: When it comes to information that can be retained for the capability, that includes information such as passport information, State driver licence information and the series of currently identified databases, but it also includes just a generic facial identification and photographic information.

Mr RICE: What it allows for, and you see in our bill the definition of "identification information", that is the range of information that is attached in the ordinary course of events to a credential. Your driver licence will have metadata behind it, which goes to things like name, date of birth and some other elements. What we allow is for that data to be collected. It goes back to the question I answered previously. If we are doing a verification we want to get to the record, no question that we are hitting more than one record, we want the record.

Mr DAVID SHOEBRIDGE: It is clause 5 (1) (m) which has "identification information about an individual is any of the following". I will not do (a) to (l).

Mr RICE: That would take a while.

Mr DAVID SHOEBRIDGE: But (m) is "a facial image of the individual".

Mr RICE: Yes.

Mr DAVID SHOEBRIDGE: Would that allow you to scrape Facebook for facial images and include them in a Commonwealth database?

Mr RICE: No.

Mr DAVID SHOEBRIDGE: Why?

Mr RICE: This is all about—

Mr DAVID SHOEBRIDGE: "Any facial image" is what it says.

Mr RICE: —us accessing existing data holdings.

Mr DAVID SHOEBRIDGE: But (1) (m) does not say where that information comes from. It just says, "identification image can include a facial image of the individual." It does not say where the information comes from. There is no limit on where they can get it.

Mr RICE: We have no plans at all to do what you are suggesting?

Mr DAVID SHOEBRIDGE: You have no plans, but a facial image you scrape from Facebook would fit the definition of identification image in 5 (1) (m)? Mr Webber has been sworn in.

Mr WEBBER: The system only operates with the information it gets from somewhere else. It may be the passport, the kind of information that the Commonwealth already holds, or it may be some state-based information that the States hold, the driver licence photos.

Mr DAVID SHOEBRIDGE: What about if the Australian Federal Police scrape facial images from Facebook or the NSW Police Force or another crime agency; that would be all thrown out?

Mr WEBBER: That would not be images that are in the inter-operability hub. They would be images that the law enforcement agency holds for its own purposes.

Mr DAVID SHOEBRIDGE: What is the purpose of 5 (1) (m) then?

Mr WEBBER: It defines what identification information is and thereby it defines what kind of information can be used in the inter-operability hub.

Mr DAVID SHOEBRIDGE: Mr Rice, before my time expired in the earlier round you were keen to tell me yes or no whether or not bundled consent as I described to you was adequate consent for an individual under the proposed 7 (3) (b). I am giving you that opportunity to answer that question.

Mr RICE: I would still say that we will work with our Federal and State colleagues to get in place appropriate consent arrangements. We will govern through, as the previous witnesses said, through the participation agreements the nature of consent that needs to be gathered from users of the system.

Mr DAVID SHOEBRIDGE: Mr Seedsman, given the very deep concerns that many people have with the way that banks have been dealing with private information, as exposed in the royal commission, are you satisfied that the banks will not misuse the information they get about New South Wales drivers and driver licences through this capability?

Mr SEEDSMAN: I do not know that I can answer that, but I can say I am not aware of any instance where RMS allows or discloses personal information to third parties based solely on the customer's consent. It would require an express legal right to do that.

Mr DAVID SHOEBRIDGE: Your agency, if the legislation passes and Commonwealth legislation passes, is about to hand over all the information you have to the capability. We know, we have heard today, that banks amongst other private entities will have access through the facial verification service. Given the concerns raised about the integrity of banks during the royal commission are you satisfied that there are adequate protections?

Mr SEEDSMAN: A bank would have to make an application to RMS for access to RMS's data. It is not a foregone conclusion that they would have access to RMS data.

Mr DAVID SHOEBRIDGE: Mr Rice, is it intended that if a bank in Queensland, for example, wants to identify an individual and get a facial verification service that if part of that individual's information is contained in a New South Wales database there would have to be an express consent from New South Wales before that information could be put through the hub?

Mr RICE: My understanding is that the bill before the Committee is about providing the legal basis for that to occur. Beyond that we would be requiring the bank in Queensland to capture consent in a form agreed by the parties to the face matching services, which is all the governments.

The CHAIR: A bank would not directly access this system?

Mr RICE: No.

The CHAIR: It would have to have a lawful purpose and specific purpose to access a specific request, which is this person?

Mr RICE: That is right.

The CHAIR: They are not tapping into the hub asking, "What can we find out about this person?"

Mr RICE: No, they have the ability to pose a query. They have already captured the sensitive personal information and they have the ability to query the system and receive a yes or no answer. They do not receive that my mum's maiden name was X, they just get a yes or no answer.

The CHAIR: Is this photo this person?

Mr RICE: Yes.

The Hon. LYNDA VOLTZ: They do not do it to you, they do it to their own private operator that has the information, their own agent.

Mr RICE: In some instances it is true, it is through that agent. But, once again, as things operate with the document verification service we have contractual arrangements in place that dictate what each of the parties need to do in terms of collecting consent.

Mr DAVID SHOEBRIDGE: Private bank, private agency, the information is routed through two private entities?

Mr RICE: Essentially.

The Hon. DAVID CLARKE: Mr Rice, what protections are available to protect images of those under the age of 18?

Mr RICE: There are restrictions in the governance arrangements and the access policies about the ability to query an image of someone under the age of 18. In the case of querying someone under the age of 18 for a law enforcement purpose there are extra authorisation measures that are put in place within police agencies to access those images.

The Hon. DAVID CLARKE: There have been a number of instances of those under the age of 18 being apprehended for planning terrorist related events.

Mr RICE: Yes. The controls we have around the face identification service, if we do not know who that person is and there is an identification query required, what is needed is an authorised officer within the agency in question. That would be a police or security agency. And the agreement has been that it would be a commissioned rank in the police service. That is a step up in terms of the oversight for the use of the service.

The Hon. DAVID CLARKE: Mr Seedsman, will licence holders under the age of 18 be uploaded?

Mr SEEDSMAN: Yes.

The CHAIR: Mr Rice, I have one question about consultation with the Australian Information Commissioner. Has there been consultation?

Mr RICE: Exhaustive and very productive. As Ms Gavel said with State privacy commissioners in I74 we learnt a lot of lessons through the Document Verification Service: consult early, privacy by design, do your PIAs, involve the Federal and State privacy regulators in that process. And that is what we have done.

The CHAIR: That finishes our session today. Thank you for providing written submissions on such short notice.

(The witnesses withdrew)

CORRECTED

(The Committee adjourned at 16.00)