Australian Government
Department of Home Affairs

Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018

Questions on Notice

Index	
QoN No.	Title
IMB/001	Prescribed by the rules
IMB/002	Transparency to the public
IMB/003	Expand ASD's remit
IMB/004	Issues raised in AHRC and LCA appearances at hearing
IMB/005	Data that's in the system
IMB/006	Interoperability hub exempted from the Privacy Act/Privacy Principles
IMB/007	Text of the amendments to the Identity-Matching Services Bill 2018
IMB/008	Biometrics Commissioner

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 03 May 2018

HOME AFFAIRS PORTFOLIO

IMB/001 - Prescribed by the rules

Asked:

Mr BYRNE: In the section the chair has helpfully pointed out, you have with all of the agencies that can access it 'an authority prescribed by the rules', which could mean a local government.
Mr Mcglynn: That is prescribed by the rules. But there are also limitations on the authority, which is the secretary. Is that right? Sorry, I will take that one on notice.

Answer:

The answer to Mr Byrne's question is no - a local government authority could not be provided access to the Face Identification Service (FIS).

Subclause 8(3) of the Identity-matching Services Bill 2018 provides that, before prescribing an authority for the purpose of paragraph 8(2)(q), the Minister must be satisfied that the authority has one or more of the functions that used to be functions of an authority described in any of paragraphs 8(2)(g) to (p). Paragraphs 8(2)(g) to (p) set out the state and territory agencies that have access to the FIS – namely state and territory police agencies and anti-corruption agencies.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 03 May 2018

HOME AFFAIRS PORTFOLIO

IMB/002 - Transparency to the public

Asked:

Mr DREYFUS: So there is no transparency to the public?
Ms Fernandez: The public are giving consent when they do it. There's transparency in that it cannot happen unless I say, 'Here is my consent.'
Mr Rice: Mr Dreyfus, I would probably take it on notice just to check about the transparency of those documents. I just can't recall what we do with DVS at the moment and whether they are on the website. I'd be happy to take that on notice.

Answer:

The Department of Home Affairs (Home Affairs) manages the Document Verification Service (DVS) on behalf of the Commonwealth and state and territory governments, under the auspices of the National Identity Security Strategy.

The DVS provides the ability to verify information on a range of Commonwealth and state and territory government issued documents, details of which are available online at www.dvs.gov.au.

This website also includes the DVS Commercial Service Access Policy and Guidelines which set out the criteria that private sector organisations must meet in order to be eligible to access the DVS commercial service. Amongst these criteria is a requirement to obtain a person's consent before using their personal information in conducting a DVS check. Private sector DVS users must agree to be subject to independent audits of their use of the system, to help ensure compliance with these requirements for use of the service. The Business User Terms and Conditions of Use, also available on the website, provide more detail on the conditions of private sector access to the DVS.

Government agencies using the DVS must also obtain a person's consent to do so. These agencies are required to provide the Department with annual compliance statements evidencing their compliance with this and other requirements for use of the service.

In relation to private sector users, the Department has a DVS Compliance Plan which outlines its approach to monitoring compliance with the terms and conditions for their use of the service, which includes an annual audit program. This plan is supported by a DVS Commercial Service Suspension and Termination Policy which provides guidance on the process that can be used to suspend or terminate access to the service as a result of business users breaching the terms and conditions for DVS use.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 03 May 2018

HOME AFFAIRS PORTFOLIO

IMB/003 - Expand ASD's remit

Asked:

Mr DREYFUS: You're a deputy secretary, but you've got no idea whether the Department of Home Affairs has got a proposal to expand ASD's remit?
Mr BYRNE: When you first answered that you also said, 'currently' in the second part of how you answered the question. You said, 'Nothing,' and then you said, 'currently'. So was there something in the past?
Ms Fernandez: I think that's a matter for the government. Currently I'm not aware—and it's not my responsibility—of any changes that are being proposed.
Mr DREYFUS: Can you take it on notice for us and ask the secretary, who I assume does have some knowledge of it?
Ms Fernandez: I'll take it on notice.

Answer:

I refer the Committee to the joint media statement issued by the Secretary of the Department of Home Affairs, the Secretary of the Department of Defence, and the Director of the Australian Signals Directorate (ASD) on 29 April 2018. The media statement confirmed that there is no proposal to increase the ASD's powers to collect intelligence on Australians or to covertly access their private data.

The statement is available in full at https://www.homeaffairs.gov.au/News/Pages/asd-powers.aspx.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 03 May 2018

HOME AFFAIRS PORTFOLIO

IMB/004 - Position of the Victorian government.

Asked:

Mr DREYFUS: Thank you. I will ask this generally because I'm conscious of the time. There have been a lot of questions by the Law Council and by the Human Rights Commission. I'm going to ask you a couple of questions about the position of the Victorian government. Assuming that we're going to wind up this hearing quite shortly, are you able to take on notice and come back to us in writing—you'll be given access to the Hansard of not only your own evidence but the evidence that has been given, and you've got of course the written submissions from the Human Rights Commission and the Law Council—the matters that they raised?
Ms Fernandez: Certainly.

Answer:

The Department has reviewed the hearing transcript and considers that issues raised by the Australian Human Rights Commission and the Law Council of Australia are addressed by the Department's original and supplementary submissions to the inquiry, its appearance at the hearing, and its responses to questions taken on notice at the hearing.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 03 May 2018

HOME AFFAIRS PORTFOLIO

IMB/005 - Data that's in the system

Asked:

Mr DREYFUS: Is it possible for either department to provide this committee with what's currently available in terms of the data that's in the system or about to be in the system or would be in the system if this bill becomes law? In addition—I'm looking for some concreteness here—provide a list of the uses that can currently be made of data that would go into the system. I've understood you to say that there are a whole lot of envisaged uses, but they are presently not the subject of any legislative arrangement and not the subject of governmental permission. You've just given the example, Mr Rice, of the ACT withholding its data and saying it does not wish to use this proposed centralised system for the purpose of a face identification service. I think I have that right—not the face verification service. Is it possible for the departments—particularly Home Affairs, which is going to run this system—to provide us with both of those things: what's going to go in it and what uses are available now? Perhaps there's a third thing—thinking aloud: what does the government envisage are future uses? A lot of the trouble—and it's apparent from the way in which the submissions have been put before us—is simply doubt on the part of members of the public. You, as the public servants responsible for this, have a very firm idea about it all, but we're looking for some way in which this committee could get at what's actually proposed and what's actually happening now. It wasn't news to me, but it probably would be news to most Australians to know that there's even a document verification service. Compared to the technology that we now have in mind, it's a pretty benign activity to compare a copy of a document with another. This is a whole different exercise. I ask you again to take that on notice. I finish there.

Answer:

Under the *Intergovernmental Agreement on Identity Matching Services* (IGA) of 5 October 2017, the Commonwealth and the states and territories agreed to share, via new face matching services, identification information used in the following evidence of identity documents; Australian passports, ImmiCards or visas; Australian citizenship certificates; driver licences; and state or territory identity documents as determined by the states.

The Department of Foreign Affairs and Trade (DFAT) is responding separately to the Committee on how Passport images are currently used by authorised agencies and how they will be used in the future through the face-matching services.

Visa and citizenship information will be drawn from a facial recognition database operated by the Department of Home Affairs (Home Affairs).

This information is currently able to be shared with a range of agencies for law enforcement and other purposes, in accordance with relevant legislation including the *Migration Act 1958* (the Migration Act), *Australian Citizenship Act 2007*, *Australian Border Force Act 2015* and the Privacy Act. For example, under the Migration Act Home Affairs can disclose identifying information for a range of purposes, including for the purpose of data-matching in order to identify or authenticate the identity of, a person.

Driver licence images will be drawn from a new national facial recognition database, known as the National Driver Licence Facial Recognition Solution (NDLFRS). The NDLFRS will hold copies of driver licence images that will continue to be held in the local systems of state and territory road agencies. In addition to supporting the sharing and matching of these images between law enforcement and other agencies, the NDLFRS will also enable road agencies to use the facial recognition technology within the system to analyse their own data using the FRAUS.

With this in mind, some states and territories have indicated the intent to include images from other document types (for example, proof of age cards or marine licences) within the NDLFRS, without necessarily sharing these with other agencies. This is why the IGA and Identity-matching Services Bill 2018 (the Bill) allow for, but do not require, the use of information from these additional document types in the face matching services.

Current arrangements for the sharing and matching of driver licence images vary across states and territories. In some cases, state and territory police are able to access local Road Agency systems, under controlled conditions. The Western Australia Police Service operates a facial recognition system used for driver licence images on behalf of that state's Road Agency. The sharing of driver licence information is conducted in accordance with relevant state and territory legislation which generally includes driver licencing and privacy laws.

As explained in the Explanatory Memorandum to the Bill, it does not seek to amend, expand or replace the legal authority that agencies other than Home Affairs rely on for information-sharing through the services. The Bill only authorises Home Affairs to collect, use and disclose identification information, for the purpose of developing and providing the services. Other agencies using the services, or making their data available through the services, will need to rely on an existing or new legal basis to share identification information with other agencies through the services. Agencies will need to provide information about their legal basis to share information through the services at the time that they enter into the legal agreements that will govern access to the services.

Clause 6 of the Bill limits the activities for which information sharing through the services can occur. These activities largely reflect the agreed purposes for information sharing set out in the IGA. The provision of the Face Identification Services (FIS) is further restricted to a subset of those activities (see

paragraph 8(1)(b) of the Bill). The activities in the Bill are the full range of possible activities for which Home Affairs will be authorised to provide the services, however the Bill does not require any agency to make their data available for all of those activities.

Each agency making data available through the services (namely Home Affairs in relation to visa and citizenship data, DFAT in relation to passport data, and each state and territory road agency in relation to data provided into the NDLFRS) will be able to further restrict the activities for which they make their data available for policy reasons, or based on restrictions in their legal authorisations to share information. These agency-specific restrictions will be set out in data-sharing arrangements to be put in place under the overarching Participation Agreement that will govern participation in the services.

Home Affairs has previously provided Parliament with examples of prospective uses of the two key services, the FIS and the Face Verification Service (FVS), in response to a question on notice from Senator Ludlam following a Senate Estimates hearing on 20 October 2015. The following information is largely drawn from that answer and may assist the Committee in understanding some of the uses of the services.

The FVS will enable agencies to verify a person's identity by searching or matching their photo (on a one-to-one basis) against an image on one of their government records. The FVS will enable three distinct functions for different users, depending on their functions and access rights.

All participants, including government agencies, local government authorities and private sector users, would have access to:

1. *Verify Subject Request* - This function will take a person's evidence of identity (EOI) document type, EOI document number and facial image (and optionally date of birth) in the request and return a simple 'Match' or 'No Match' response from the data-holding agency indicating whether there was a biometric match (based on an agreed threshold) against the person's corresponding record.

   This could be used, for example, where a person provides a driver's licence as evidence of their identity to apply for a passport. The FVS could enable the passport office, on a risk management basis, to ask the road agency to confirm that the photo on the application matches the photo held on their record.

Government agencies such as law enforcement and regulatory agencies will have access to two additional functions, subject to need and access rights:

2. *Retrieve Facial Biometric* - This function will take a person's EOI document type, EOI document number (and optionally date of birth) in the request and return a response from the data-holding agency with a facial image and, if needed and authorised, biographic details from the person's corresponding record.

   This could be used by a law enforcement agency to confirm that an EOI document presented by a person is not fraudulent (i.e. that the document does not contain a substituted photo with otherwise 'legitimate' biographical information of another person).

3. *Search Subject Request* - This function will take a person's first name, last name, date of birth and facial image in the request and return a response from the data-holding agency with the facial image from the person's corresponding record. In the event that there is more than one corresponding record with the same first name, last name and date of birth, the response will only indicate that there are multiple records.

   This could be used by a law enforcement agency to confirm, in the absence of an EOI document, that the claimed identity of a person who is suspected to have committed a criminal offence matches that on one of their government records.

Local government authorities and non-government entities will not have access to these two functions.

A limited number of national security, law enforcement and anti-corruption agencies will have access to the FIS in addition to the FVS. These agencies are specifically listed in subclause 8(2) of the Bill. Other agencies not listed in the Bill, as well as local government authorities and non-government entities, will not have access to the FIS.

The FIS will enable agencies to match a photo of an unknown person against multiple government records (on a one-to-many basis) to help establish their real identity, or to detect where a person may hold multiple fraudulent identities.

The FIS will enable two distinct functions:

1. *Identify Subject Request* - This function will take a facial image and *mandatory* demographic details (age range and gender) in the request, and return a response from the data-holding agency with the most likely image match or matches (based on a pre-configured threshold/s) and, if needed and authorised, associated biographic data.

   This could be used, for example, where a law enforcement agency arrests a member of a child exploitation ring and seizes a number of computers that contain child exploitation material, including images of a suspected offender. The agency could submit a facial image and demographic details of the suspect and seek to match it against one or more government identity holdings (e.g. passports and/or driver licences) to establish their identity.

2. *Advance Identify Subject Request* - This function will take a facial image and *optional* demographic and/or partial biographic details in the request, and return a response from the data-holding agency with the most likely image match or matches (based on a pre-configured threshold/s) and, if needed and authorised, associated biographic data.

   This could be used, for example, where a terrorist cell has bombed a metropolitan office building and has threatened further attacks. A CCTV has captured the facial image of one of the suspected terrorists performing reconnaissance on the office building two days earlier. A specialist counter-terrorism team could submit the facial image to seek a match against several

government identity holdings (e.g. passports, visas and driver licences) to determine the suspect's identity.

Staff from the agencies listed in subclause 8(2) that access the FIS will be specifically trained in facial image comparison and all match results will be assessed by an officer – there will always be a 'person in the loop'.

A publically available factsheet on the Department of Home Affairs website, provides some more information about the services and may assist the Committee to understand how the services will operate. A copy of the factsheet is attached for the Committee's information.

Australian Government
Attorney-General's Department

Face Matching Services

FACT SHEET – FACE MATCHING SERVICES

The Australian Government is working with states and territories to implement new biometric face matching services. These services have been developed to protect Australians from identity crime, and provide law enforcement and security agencies with a powerful new investigative tool to stay one step ahead of terrorists and criminals that seek to circumvent Australia's identity checking processes.

On 5 October 2017, the Prime Minister and state and territory leaders signed an *Intergovernmental Agreement on Identity Matching Services*. Under the Agreement, agencies in all jurisdictions will be able to use new Face Matching Services to access passport, visa, citizenship, and driver licence images – while maintaining robust privacy safeguards.

The use of the Face Matching Services will:

- protect people from identity theft, and help victims restore their compromised identities
- prevent criminals and terrorists creating and using fraudulent identity documents
- assist police to investigate other serious criminal activity
- help people to prove who they are when using government services online.

Face Verification Service (FVS)

The FVS is a one-to-one image based verification service that can match a person's photo against an image on one of their government records, such as a passport photo, to help verify their identity. Often these transactions will occur with the individual's consent.

For example, where a person uses their citizenship record as evidence of their identity to apply for a passport, the system could enable the passport office to ask the Department of Immigration and Border Protection to confirm the identity of the passport applicant.

Face Identification Service (FIS)

The FIS is a one-to-many image based identification service that can match a photo of an unknown person against multiple government records to help establish their identity. Access to the FIS will be restricted to agencies with law enforcement or national security related functions.

Police will use the FIS for investigations of more serious offences. For example, it may be used to identify a suspected paedophile from child exploitation material, or to identify an armed robber from a still image taken from CCTV footage. It will not be used for minor offences such as littering or parking infringements, but it may be used to help identify victims of disasters and to locate missing persons.

Access to the FIS will only be provided to a limited number of users in specialist areas with training in how to interpret the results. It does not provide for fully automated or 'real time' surveillance of public spaces, but does enable more targeting searching using still images, taken from CCTV for example, to quickly identify a 'person of interest' for public safety purposes.

Why these services are necessary

The Australian Government is investing in this new system to help combat identity crime, which is one of the most common crimes in Australia and costs around $2.2 billion per year. Around 1 in 20 Australians experience identity crime each year that results in financial loss.

Identity crime is a key enabler of serious and organised crime, such as drug trafficking, money laundering, people smuggling, child exploitation and terrorism. Australians convicted of terrorism offences have used false names to avoid detection while planning attacks. This includes purchasing ammunition and chemicals to make explosives and pre-paid mobile phones to communicate anonymously.

An operation by the joint Australian Federal Police and New South Wales Police Identity Security Strike Team found that around 1,700 fraudulent identities seized from just one criminal syndicate were linked to:

- 29 high profile criminals linked to historic or ongoing drug investigations
- more than $7 million in fraud against individuals and financial institutions, and
- more than $50 million that was laundered offshore and was likely to be proceeds of crime.

While existing measures such as the Document Verification Service (DVS) are helping to prevent the use of fake identity documents, criminals are now producing high quality fraudulent identity documents. These false documents contain personal information stolen from innocent and unknowing victims, but with someone else's photo – documents that would pass a DVS check. Preventing this type of fraud can be assisted by greater use of biometrics, such as the FVS and FIS.

How the system works

The Face Matching Services draw on existing collections of images that are used by government agencies for issuing evidence of identity documents. But there is no single database that will hold all passport, visa, citizenship and driver licence images.

A central Hub or exchange facilitates data sharing between agencies on a query and response basis, without storing any personal information. This enables better auditing and oversight, while maintaining data sources separately.

Passport, visa and citizenship images will continue to be held by the Commonwealth agencies that issue these documents, and that already have facial recognition systems.

Driver licence images will be made available via a common facial recognition system, hosted by the Commonwealth on behalf of participating state and territory driver licencing agencies.

This is the most cost effective way of providing access to these images as not all states and territories currently use facial recognition for their driver licence images – which can leave them more susceptible to fraud. The system will provide additional face matching services for states and territories to help improve the integrity of driver licence data holdings.

Data contributed by the states and territories will remain under their control. The Commonwealth will not have direct access to this information - access will only be provided in accordance with data sharing agreements with the states and territories.

Why legislation is needed

A range of legislation already authorises the sharing of facial images for law enforcement purposes and other purposes.

New Commonwealth legislation is needed to authorise the collection, use and disclosure of driver licence information via the central driver licence database. This legislation will not increase the powers of police agencies to collect this information, or to use information in ways that they are not already authorised to do. It will provide a more transparent basis for the Commonwealth to operate the driver licence database, with additional privacy safeguards.

Security and privacy protections

The system will adopt best practice security and access arrangements in accordance with the Government's Protective Security Policy Framework and the Information Security Manual, and will be subjected to independent penetration and vulnerability tests as well as an independent security review by the Australian Signals Directorate.

The central infrastructure will exchange messages but it will not conduct any matching nor store any personal information. This approach allows individual agencies to retain full control over their own image holdings and decisions about the organisations with which they share this information.

The driver licence component of the system will be hosted separately and remain under the control of participating states and territories. The Commonwealth will not have direct access to this information - access will only be provided in accordance with data sharing agreements with the states and territories.

Participating agencies will require a lawful basis to collect and use facial images, just as they do now.

The system will have robust privacy safeguards, informed by independent privacy impact assessments conducted throughout the design and implementation phases, in consultation with the Australian Privacy Commissioner. These assessments will be published wherever possible, so that the community can see the safeguards that are being built into the system.

Participating agencies will need to enter formal data sharing agreements containing safeguards for the sharing and use of personal information, and regular audits will help ensure that these protections are functioning properly. Agencies will continue to be subject to independent oversight by a range of existing external bodies such as privacy commissioners, ombudsmen and anti-corruption or integrity commissioners for their use of personal information. The operation of the system will be audited by the Office of the Australian Information Commissioner.

For more information contact the Attorney-General's Department at identity.security@ag.gov.au

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 03 May 2018

HOME AFFAIRS PORTFOLIO

IMB/006 - Interoperability hub exempted from the Privacy Act/Privacy Principles

Asked:

Are there instances where uses of any of the identity-matching services via the interoperability hub are not covered by, or are exempted from, the Privacy Act/Privacy Principles?

Explanation for assistance
I note that Section 8(2) provides for a large number of entities that may request the provision of the FIS which includes:

- Australian Border Force;
- the Australian Commission for Law Enforcement Integrity;
- the Australian Crime Commission;
- the Australian Federal Police;
- the Australian Security Intelligence Organisation;
- a Department administered by a Minister administering any of the following Acts:
- the Australian Citizenship Act 2007;
- the Australian Passports Act 2005;
- the Foreign Passports (Law Enforcement and Security) Act 2005;
- the Migration Act 1958
- a police force of a State or Territory;
- Commissions against corruption (however named) in:
  - New South Wales;
  - Victoria;
  - Queensland;
  - Western Australia;
  - South Australia;
  - Tasmania; and
  - The Northern Territory.

It may be that parts of the legislation establishing the above bodies or legislation mentioned above exempts the agency/body from the Privacy Act/Privacy Principles. It is this situation as well as any others where uses of any of the identity-matching services via the interoperability hub are not covered by or are exempted from the Privacy Act/Privacy Principles that this question goes to.

Answer:

The Commonwealth *Privacy Act 1988* (the Privacy Act) contains full exemptions for some agencies, and contemplates a range of circumstances in which other agencies can utilise exceptions to certain specific requirements in the Australian Privacy Principles (APPs) in their handling of personal information. These include, for

example, exceptions to the requirement to obtain consent where the collection, use or disclosure of information is authorised by law or is in the course of a law enforcement-related activity. Agencies may rely on these exemptions or exceptions, where applicable, when using the face-matching services.

The Privacy Act does not apply to state and territory agencies. However, most states and territories have equivalent privacy legislation that applies to agencies in those jurisdictions. Agencies in South Australia and Western Australia are not subject to privacy legislation, as no comprehensive privacy legislation exists in those jurisdictions. However, under the legally binding Face Matching Services Participation Agreement, these agencies will be required to agree to be subject to the APPs in relation to their use of the face-matching services.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 04 May 2018

HOME AFFAIRS PORTFOLIO

IMB/007 Text of the amendments to the Identity-Matching Services Bill 2018

Asked:

The Committee has asked for the text of the amendments to the Identity-Matching Services Bill 2018 envisaged in Minister Dutton's response to the Scrutiny of Bills Committee.

Answer:

The text of these amendments is currently under development.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 03 May 2018

HOME AFFAIRS PORTFOLIO

IMB/008 – Commonwealth Biometrics Commissioner -

Asked:

Mr DREYFUS: The committee is indebted to you for that and for the supplementary submission that's coming. I'll raise the points made by Victoria. We've got a submission from the Office of the Victorian Information Commissioner and we've got, somewhat unusually, a separate submission from the Victorian Special Minister of State, who has got ministerial responsibility for this kind of matter. Specifically, the Victorian Special Minister of State has suggested—and this goes to the point of safeguards and oversight—that consideration ought to be given to a separate integrity figure. I don't think that the person is given a name, but it would be something like 'Commonwealth Biometrics Commissioner'. The Victorian minister refers to the Office of the Biometrics Commissioner in the UK and notes that there's another commissioner called the UK Surveillance Camera Commissioner. I invite the department to respond to that suggestion. Specifically, the Victorian minister expresses concern that this Identity-matching Services Bill is inconsistent with the intergovernmental agreement. Have you had a chance to look at the comments made by the Victorian minister?

Answer:

The Department has addressed the matter of a Biometrics Commissioner on page 9 of our supplementary submission (submission 12.1).