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**
IMS/009	ACIC BIS contract
IMS/010	Victorian Government Submission
IMS/011	Privacy Act 1998 - Exemptions
IMS/012	Annual reporting of accuracy testing – Smart gates
IMS/013	Definition of National Security
IMS/014	Department's position regarding subordinate legislative instruments
IMS/015	Privacy and security safeguards
IMS/016	Privacy protections - Participation and Access Agreement
IMS/017	Privacy provisions
IMS/018	Approval of state and territory government IMS requests
IMS/019	Recourse - Consistency with Privacy Act and APPs
IMS/020	Auditing and Oversight - s7(4)
IMS/021	Redrafting of provisions
IMS/022	Awareness of use of images
IMS/023	Authorisation for access
IMS/024	Disclosures of information
IMS/025	Disallowable instruments
IMS/026	Data breaches
IMS/027	Reporting of security incidents

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/009*) – ACIC BIS contract -

Asked:

Are there any performance issues to be learnt (or have been learnt) from the announcement on 5 June 2018 by the Australian Criminal Intelligence Commission (ACIC) that it had decided to discontinue its Biometric Identification Services (BIS) project?

Answer:

The Australian National Audit Office is conducting an audit into the project, as requested by the ACIC in February 2018.

The Department of Home Affairs (Home Affairs) will consider the outcomes of this audit when they are available to determine if there are any lessons that can be applied to the implementation of the face matching services.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/010*) – Victorian Government Submission

Asked:

Can the Department of Home Affairs respond in writing to the issues raised in the Victorian Government submission to the inquiry?

Answer:

Many of the issues raised in the Victorian Government's submission to the inquiry relate to differences between the Bill and the policy position of the Victorian Government or the legal authority Victorian government for sharing information through the services; not to inconsistencies the Bill and the *Intergovernmental Agreement on Identity Matching Services* (IGA).

To the extent which there are differences between the Bill and Victoria's position, this is because in order to facilitate the provision of identity-matching services involving all states and territories, it is necessary for the Bill to capture the full range of data-sharing contemplated by each of those jurisdictions.

For example, some states and territories have indicated that it will be necessary for the National Driver Licence Facial Recognition Solution (NDLFRS) database to hold information used for different types of licences, such as marine and firearm licences. This is clearly contemplated by clause 6.18 of the IGA and is because it is not feasible for those jurisdictions to separate this information from their driver licence data. As such, the Bill must capture this to ensure the Department of Home Affairs (Home Affairs) has legal authority to collect this information from and for those states.

However, nothing in the Bill requires any state, territory or Commonwealth agency to make any data available through the services, or to make it available to particular users (for example, private sector or local government authorities). As agreed under the IGA, data-holding agencies retain control over what data they will share through the services, and to which users, subject to their legal authority.

The Victorian Government retains control over what data it will provide into the NDLFRS database, and to what extent that data is shared and with whom through the services. These arrangements will be set out in the supporting agreements between data-holding agencies and participating agencies wishing to use the services. This applies equally to any new types of identification information or new identity-matching services that may in future be prescribed in the rules.

Private sector access

In relation to private sector use, the Victorian Government submission incorrectly asserts that the Bill allows the private sector to access *any* of the face matching services. This is not accurate. The Bill defines each of the identity-matching services separately in clauses 8 to 12. In each case, the Bill defines what the service involves, including who makes the request. Clause 10 which relates to the Face Verification Service is the only definition which permits requests by non-government entities (see subclause 10(2)).

The Victorian Government submission also suggested that paragraph 7(3)(d)(ii) of the Bill refers to non-government entities (private sector users) in addition to local government authorities. As currently drafted, the Bill requires non-government entities to be subject to the Privacy Act in order to access face-matching services (subparagraph 7(3)(d)(i)). Adding non-government entities to subparagraph 7(3)(d)(ii) as suggested by the Victorian Government would reduce the efficacy of this requirement by allowing private sector organisations to be bound by another law or an agreement with Home Affairs.

Home Affairs' position is that all non-government entities wishing to access the FVS should be bound by the Privacy Act, including by opting-in to the Privacy Act in accordance with the process provided for by the Office of the Australian Information Commissioner if they are not automatically subject to the Privacy Act (i.e. organisations with an annual turnover of less than $3 million).

Governance of the IMS and provision of biometric capability

The Victorian Government submission raises concerns about the adequacy of the governance and oversight arrangements for the face matching services, and; *"particularly note that aside from an Annual Reporting cycle (cl. 28), there are no provisions in the IMS Bill to support timely reporting, including misuse of data or access breaches by users of the IMS itself."*

Home Affairs addressed issues relating to governance, oversight and annual reporting in paragraphs 38 to 58 of its supplementary submission.

Management of data breaches is governed by the new data breach notification provisions in Part IIIC of the Privacy Act, which will apply to the NDLFRS database hosted by Home Affairs. It is not necessary to duplicate data breach reporting by requiring this information to be included in the annual report under the Bill.

In relation to other matters, such as security incidents and unauthorised use or disclosure of information, reporting on these issues may not always be appropriate, for example; if it would disclose information about the security architecture of the systems. However, this information will be able to be captured, and properly investigated and assessed, through annual audit requirements on participating agencies using the services, and the various reviews of the services required under the IGA (every three years), and the Bill (a review to be commenced within five years). These mechanisms provide a more appropriate opportunity to consider these issues in detail and identify options to address them.

The Victorian Government submission also suggested that the Commonwealth consider establishing a Biometrics Commissioner to oversight the face-matching services. Home Affairs notes that the role of the UK Office of the Biometrics Commissioner primarily relates to reviewing the retention and use by the police of DNA samples, profiles and fingerprints, and police use of facial biometrics. The Bill is not seeking to expand the circumstances in which police can collect biometric information from individuals, or govern their use or retention of biometric information. The Bill will enable Home Affairs to facilitate information-sharing between agencies that already have a legal basis to do so. The extent to which existing or future police powers in relation to biometric information may require greater oversight is a separate issue, outside the scope of the Bill.

Agencies participating in the identity matching services will continue to be subject to existing oversight arrangements that apply to their activities or functions. At the Commonwealth level, this includes the Inspector-General of Intelligence and Security (for intelligence agencies), the Office of the Australian Information Commissioner, and the Commonwealth Ombudsman. Comparable oversight bodies also operate at the state and territory level.

Consent and notification

The Victorian Government submission raises questions about how citizens will be appropriately informed of the use of their driver licences in the face matching services, and how consent will be obtained.

State and territory road agencies will have the primary responsibility for notifying their clients of the use of clients' driver licence information in the NDLFRS. This information will be provided to the Commonwealth, as the host of the NDLFRS, in accordance with relevant state and territory laws.

Private sector and local government use of the FVS will be on similar terms to those that operate in relation to the Document Verification Service (DVS), which has been operating for approximately 10 years as a consent-based service.

Governance of the DVS involves robust contractual arrangements and a comprehensive program of independent audits of users of the services. These same arrangements will apply to private sector and local government access to the FVS.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/011*) – Privacy Act 1998 - Exemptions

Asked:

Can the Department of Home Affairs provide an explanation of how the Privacy Act 1988 will apply to the operation of the services enabled by the Bill, taking into account the exemptions that apply to some of the key users and uses of the services.

Answer:

Operation of the services by the Department of Home Affairs

The purpose of the Identity-matching Services Bill 2018 (the Bill) is to provide an authorisation under law for the Department of Home Affairs (Home Affairs) to collect, use and disclose identification information in order to establish and operate the systems that support the face matching services and deliver the services through those systems. The term 'identification information' is defined in the Bill, and captures a range of information that is characterised as 'personal information' (including 'sensitive information') under the *Privacy Act 1988* (the Privacy Act).

The Australian Privacy Principles (APPs) govern the collection (APP3), use and disclosure (APP6) of personal information. APP3 and APP6 provide for circumstances in which agencies can collect, use and disclose personal information. These include, relevantly, where the collection, use or disclosure is authorised by or under an Australian law (APP3.4 (a) and APP6.2 (b) respectively). The Bill will provide authorisations for this purpose.

This will mean that Home Affairs does not need to rely on other arrangements, such as obtaining consent, for the collection, use and disclosure of identification information for the purpose of providing the services. As noted in the Department's supplementary submission (at paragraph 32), relying on consent to collect identification information for the purpose of inclusion in the National Driver Licence Facial Recognition Solution (NDLFRS) database would not be feasible – it would effectively enable criminals to 'opt-out' of the face matching services. This would defeat the key objectives of the system, including the detection of fraudulent identity documents and the prevention, investigation and prosecution of criminal offences.

The Bill does not otherwise seek to affect the application of the Privacy Act to the services, or to the operation of the interoperability hub and NDLFRS by Home

Affairs. Relevant APPs such as APP1 – open and transparent management of personal information, APP5 – notification of collection of personal information, APP10 – quality of personal information, APP11 – security of personal information, APP12 – access to personal information and APP13 – correction of personal information, continue to apply.

Home Affairs will collaborate with state and territory road agencies to meet the requirements contained in these APPs, particularly as they relate to the NDLFRS database which will contain a copy of information that is held by state road agencies. Home Affairs is working with these agencies to ensure that appropriate mechanisms are in place to enable individuals to correct and access their information contained in the NDLFRS, and to notify individuals of the collection of their information for inclusion in the NDLFRS.

Use of the services by Commonwealth participating agencies

The Bill also does not seek to change the way in which the Privacy Act applies to the collection, use or disclosure of identification information by other Commonwealth agencies using the face matching services. The same privacy obligations that currently apply to agencies' handling of personal information will continue to apply to their handling of information obtained through the face-matching services; as will the existing exemptions and exceptions for certain agencies' compliance with the APPs.

Some Commonwealth user agencies are exempt from the requirements of the Privacy Act. In particular, the acts and practices of the Australian Security Intelligence Agency (ASIO), the Australian Crime Commission (now the Australian Criminal Intelligence Commission or ACIC) and the Integrity Commissioner are expressly exempted from the operation of the Privacy Act. This exemption will apply to these agencies' use of identification information obtained through the services, just as it applies to their use of personal information obtained via other means.

A key objective of the Privacy Act is to balance the protection of privacy with the interests of entities in carrying out their lawful and legitimate functions and activities. Exemptions have been included in the Privacy Act in recognition of the increased need for these agencies to be able to handle personal information in order to achieve their objectives in circumstances where the standard requirements set out in the APPs cannot or should not apply.

It also recognises the substantial protections already afforded to personal information handled by these agencies, including secrecy provisions and robust accountability frameworks including external oversight. These agencies will continue to be subject to these arrangements, including oversight by bodies such as the Inspector-General of Intelligence and Security (for intelligence agencies), the Commonwealth Ombudsman, and Parliamentary Committees.

The Privacy Act also contemplates that there are other circumstances in which certain specific requirements in the APPs should not apply. This includes exceptions from certain requirements under the APPs for collection, use and disclosure in the course of enforcement related activities undertaken by enforcement bodies. Some

users of the face matching services will be enforcement bodies that will rely on this exception to collect, use and disclose personal information through the services.

Some other user agencies will also rely on exceptions to certain APPs where they have specific legislative authority for certain activities involving the collection, use or disclosure of personal information, as they do now. This could include, for example, agencies responsible for compliance with legislative schemes such as welfare payments or tax arrangements.

In providing for these exceptions within the Privacy Act and by passing other legislation that permits handling of personal information, the Parliament has already considered the appropriateness of these provisions and the adequacy of alternative safeguards where particular APP requirements may not apply.

It is important to note that as with the operation of the services by Home Affairs, agencies which may rely on exceptions in APP3 and APP6 as the legal basis to collect, use or disclose identification information when using the services are not exempt from the other requirements in the APPs. They must continue to comply with their other obligations under the APPs in relation to their use of the face matching services, as they currently do in relation to their handling of personal information more generally.

State and territory agencies

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. Many of these have similar exceptions to some requirements for some agencies, including law enforcement agencies. These will apply to their participation in the face-matching services in the same way that they apply to their handling of personal information obtained through other means.

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 comply with the APPs in relation to their use of the face matching services as if they were an APP entity.

Private sector organisations and local government authorities

Under the Bill, all private sector organisations wishing to participate in the face matching services will need to be subject to the Privacy Act, including by opting in if they are not automatically covered (7(3)(d)(i)). These organisations will need to comply with all obligations imposed on them under the Privacy Act in relation to their participation in the services.

Local government authorities may also be bound by a law of a state or territory or enter into a written agreement with Home Affairs that provides comparable protection to the Privacy Act. For most local government authorities, this will be existing privacy legislation in their jurisdiction.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/012*) – Annual reporting of accuracy testing - Smartgates

Asked:

Are there impediments to the Department reporting annually on the results of accuracy testing?

Answer:

There are a range of factors that influence the accuracy of facial recognition systems supporting the face matching services. These include the quality of 'probe' images that are submitted as part of matching requests, the quality of 'reference' images against which the probe images are being compared, the configuration and performance of the facial recognition software and the aptitude of personnel who review the results of matching queries.

In order to report on the actual performance of the face matching services, the Department would need to obtain information on the outcome of match results from agencies which use the services. For example, information from a police service on whether the gallery of images returned in response to a Face Identification Service query contained an image(s) of the search subject, or information from an agency using the Face Verification Service on whether a 'no match' response was an error, or whether an individual was attempting to pass themselves off as another person.

The Department does not routinely collect this information, which may constitute personal information, as it is not strictly necessary to do so in order for the Department to provide the matching services. In some cases this information may also be sensitive from a law enforcement or security perspective, such as where it relates to specific investigations.

The Department conducts ongoing testing and tuning of the facial recognition software or algorithms used to support the face matching services, using Australian datasets, to continually improve the accuracy of systems supporting these services. This testing is conducted in controlled conditions designed to simulate actual use cases, but cannot necessarily provide a true indication of the actual performance of the services under 'real world' conditions.

The Department's policy is to avoid publishing technical information on the configuration or performance of biometric systems so as to avoid the release of information that could be used to test or exploit potential vulnerabilities in these systems.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/013*) – Definition of National Security

Asked:

Why does the Bill use the definition of 'National Security' from the National Security Information (Criminal and Civil Proceedings) Act 2004 rather than the definition at section 90.4 of the Criminal Code?

Answer:

In section 6 of the Bill, 'identity or community protection activity' includes conducting an investigation or gathering intelligence relevant to Australia's national security. National security is defined by reference to the definition in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (NSI Act).

The NSI Act definition is in substance almost the same as the definition of national security in section 90.4 of the Criminal Code. One difference is that "law enforcement interests" is not part of the Criminal Code definition. It is needed in the identity matching context. The NSI Act definition is used as a reference point in other legislation, for example recently in the *Security of Critical Infrastructure Act 2018.*

In the NSI Act security means Australia's defence, security, international relations or law enforcement interests (section 8). The NSI Act goes on to provide that "security" has the same meaning as it has in the *Australian Security Intelligence Organisation Act 1979* (section 9). In the ASIO Act security means:

(a) Protection from:
    (i) Espionage
    (ii) Sabotage
    (iii) Politically motivated violence
    (iv) Promotion of communal violence
    (v) Attacks on Australia's defence system
    (vi) Acts of foreign interference
(b) Protection of Australia's territorial and border integrity
(c) Carrying out Australia's responsibilities to a foreign country related to the above.

The Criminal Code definition in 90.4 is structured differently, but covers almost the same ground:

(1) The national security of Australia or a foreign country means any of the following:

(a) the defence of the country;
(b) the protection of the country or any part of it, or the people of the country or any part of it, from activities covered by subsection (2);
(c) the protection of the integrity of the country's territory and borders from serious threats;
(d) the carrying out of the country's responsibilities to any other country in relation to the matter mentioned in paragraph (c) or an activity covered by subsection (2);
(e) the country's political, military or economic relations with another country or other countries.

(2) For the purposes of subsection (1), this subsection covers the following activities relating to a country, whether or not directed from, or committed within, the country:
(a) espionage;
(b) sabotage;
(c) terrorism;
(d) political violence;
(e) activities intended and likely to obstruct, hinder or interfere with the performance by the country's defence force of its functions or with the carrying out of other activities by or for the country for the purposes of its defence or safety;
(f) foreign interference.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/014*) – Department's position regarding subordinate legislative instruments

Asked:

What is the Department’s position on what should be included in legislation as opposed to subordinate legislative instruments such as regulations?

Answer:

The Department has considered the appropriateness of using subordinate legislation on a case-by-case basis. Consideration has been given to issues such as the nature of the amendments and the legislation being amended, the need for flexibility and the importance of Parliamentary Scrutiny. During the drafting of legislation, regard is also given to advice from the Office of Parliamentary Counsel on this issue. The Department also considered relevant material and comments from the Senate Standing Committee for the Scrutiny of Bills and the Senate Standing Committee on Regulations and Ordinances.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/015*) – Privacy and security safeguards

Asked:

Has the National Security Coordination Group started on development of privacy and security safeguards in relation to the identity-matching services?

Answer:

Yes.

In accordance with clause 7.2 the Intergovernmental Agreement on Identity Matching Services (IGA), a Face Matching Services Participation Agreement (the Participation Agreement) is under development through the National Identity Security Coordination Group (NISCG) to provide a legally binding framework within which Commonwealth, state and territory agencies will share information via the face matching services.

The Participation Agreement will set out the respective roles, rights and responsibilities of participating agencies in relation to their participation in the services. The Participation Agreement is nearing completion and will be subject to final approval by the NISCG. Under the IGA, the NISCG is the officials-level body responsible to Commonwealth, state and territory ministers for the efficient and effective delivery and management of the face matching services.

The Participation Agreement will include a range of privacy and security safeguards, including requirements for agencies using the services to:

- provide a statement of legislative authority demonstrating the agency's legal basis to obtain identification information through the services;
- commission or otherwise participate in a privacy impact assessment on their use of the services (or for agencies exempt from privacy legislation, must provide a privacy statement that must be approved by the NISCG);
- adopting a Privacy Governance Framework and Management Standards to reflect its management of information flows associated with the agency's use of the services;
- obtain security accreditation and/or complete a security risk management plan in relation to systems that access the interoperability hub;

- provide training for their personnel that will have access to the services, including (where applicable) facial recognition and image comparison training;
- destroy all identification information obtained through the services after the minimum period of time necessary to both fulfil the purpose for which it was obtained and comply with any applicable laws relating to its retention of data or records; and
- be subject to annual audits on their use of the services, which will be provided to the NISCG.

The Participation Agreement will also impose obligations on Home Affairs as the operator of the interoperability hub, including to maintain security accreditation in accordance with the Protective Security Policy Framework, and obtain annual independent privacy assessments of the interoperability hub and the National Driver Licence Facial Recognition Solution (NDLFRS).

In accordance with clause 7.5 the Intergovernmental Agreement on Identity Matching Services (IGA) the NISCG will also approve a legally binding NDLFRS Hosting Agreement. This agreement will set out the privacy and security safeguards and other terms and conditions under which states and territories will provide, and the Commonwealth will host the data in the NDLFRS database.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/016*) – Privacy protections - Participation and Access Agreement

Asked:

Is it correct that most privacy protections are not included in the Bill but will be included in Participation and Access agreements?

Answer:

Privacy protections relating to the handling of personal information used in the face matching services are contained in a range of enabling legislation, including the Bill, Commonwealth, state and territory privacy legislation, other agency-specific legislation, as well as a legally-binding Face Matching Services Participation Agreement (the Participation Agreement).

The Bill contains the following specific privacy safeguards:

- restricting the types of identification information that may be collected, used and disclosed through the services (clause 5);
- limiting information sharing to a defined set of services (clauses 7-12);
- restricting the activities for which identification information can be shared through the services (clause 6);
- restricting the agencies that can access the Face Identification Service to a prescribed list of agencies (clause 8);
- limiting private sector and local government access to verification services only, with conditions on the use of these services including requirements to obtain consent and be subject to an appropriate privacy regime (subclause 7(3));
- an offence for unauthorised recording or disclosure of identification information by Department of Home Affairs staff or contractors with access to the systems that support the services (clause 21);
- annual reporting to Parliament on the use of the identity-matching services (clause 28);
- a statutory review of the operation of the Act to be commenced within five years, which must be reported to Parliament (clause 29); and
- in relation to rules that may be made under the Bill:

- a requirement for the Minister to consult the Information Commissioner and the Human Rights Commissioner before making rules providing for new types of identification information or new identity-matching services (paragraph 5(4)(b) and subclause 7(5)); and
- providing for disallowance and sunsetting of any rules made (subclauses 30(3) and (4)).

Participating agencies will continue to be subject to existing privacy obligations and oversight arrangements that apply to them under Commonwealth, state and territory privacy legislation and agency-specific legislation (see response to question IMS/011).

Participating agencies will also be subject to a range of other specific privacy requirements under the Face Matching Services Participation Agreement (see response to question IMS/015).

Through the Participation Agreement, agencies in jurisdictions that do not have privacy legislation, namely South Australia and Western Australia, will be required to comply with the APPs in relation to their use of the face matching services as if they were an APP entity.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/017*) – Privacy provisions

Asked:

Where in the Bill is privacy provided for?

Answer:

The Bill's privacy safeguards are outlined in the Department's response to the Committee's previous question (IMS/016).

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/018*) – Approval of state and territory government IMS requests

Asked:

Proposed section 7(4) provides that local government authorities and non-government entities can request an identity-matching service where they have entered into a written agreement with the Department that is comparable to the protection under the Australian Privacy Principles (APP). Who will decide whether such an agreement is comparable to the APPs?

Answer:

The Bill does not enable non-government entities to enter into a written agreement with the Department to access an identity-matching service. The use of such agreements is limited to local government authorities by section 7(3)(d)(ii) of the Bill.

The specific form of agreements between the Department and local government authorities seeking access to an identity-matching service (the purpose of which is limited to verifying an individual's identity by section 7(2)(a) of the Bill) is yet to be determined.

Section 7(4)(a) provides that such an agreement must provide for the protection of personal information comparable to that provided by the APPs.

In developing these agreements Home Affairs will consider:

- the existing oversight arrangements that apply to the authority and options available in the jurisdiction for monitoring, compliance and recourse under state laws; and
- any available guidance from the Office of the Australian Information Commission (OAIC), including Chapter 8 of the *Australian Privacy Principles Guidelines* which provides guidance on assessing whether a law or agreement provides comparable protection to the APPs.

Home Affairs will also consult with the OAIC in developing these agreements.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/019*) – Recourse - Consistency with Privacy Act and APPs

Asked:

Proposed section 7(4) provides that such an agreement must have a means for an individual to seek recourse if his or her personal information is dealt with in a way contrary to the law or agreement. How will the Department ensure that such 'means for an individual to seek recourse' are the same or similar to those provided under the Privacy Act and the APPs?

Answer:

The specific form of agreements between the Department and local government authorities seeking access to an identity-matching service, which may be developed pursuant to section 7(3)(d)(ii) and section 7(4) of the Bill, is yet to be determined.

Section 7(4)(c) provides that such an agreement must provide a means for an individual to seek recourse if his or her personal information is dealt with in a way contrary to the agreement.

In developing these agreements Home Affairs will consider:

- the existing oversight arrangements that apply to the authority and options available in the jurisdiction for monitoring, compliance and recourse under state laws; and
- any available guidance from the Office of the Australian Information Commission (OAIC), including that provided in Chapter 8 of the *Australian Privacy Principles Guidelines* which provide guidance on determining whether comparable enforcement mechanisms to those in the APPs exist in another jurisdiction.

Home Affairs will also consult with the OAIC in developing these agreements.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/020*) – Auditing and Oversight - s7(4)

Asked:

What auditing and oversight will be applied to agreements concluded in accordance with proposed section 7(4)?

Answer:

Private sector and local government access to the Face Verification Service (FVS) will be on similar terms to those that operate in relation to the Document Verification Service (DVS), which has been available to the private sector for over four years.

Governance of the DVS involves robust contractual arrangements and a comprehensive program of independent audits of private sector users of the services. This audit program has resulted in some entities' access to the service being suspended for non-compliance with DVS terms and conditions.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/021*) – Redrafting of provisions

Asked:

Could the provisions defining each of the identity-matching services be redrafted, so that their functionality is fully defined in the Bill rather than in the Explanatory Memorandum?

Answer:

The purpose of the Bill is to provide the Department with the authorisation it requires, subject to appropriate safeguards, to operate the technical systems that will support the identity-matching services.

The clauses in the Bill defining the interoperability hub, National Driver Licence Facial Recognition Solution (NDLFRS), and the identity-matching services are necessary to impose appropriate restrictions on the authorisation the Bill provides.

The Bill does not go into technical detail about how the interoperability hub or NDLFRS work. This is consistent with the approach in comparable Commonwealth legislation authorising collection, use or disclosure of personal information.

The typical approach is for an Act to authorise the Department to collect, use or disclose relevant personal information for specified purposes – not to prescribe how supporting ICT systems work.

An example is the *AusCheck Act 2007*, which authorises the collection of information and the operation of a database to retain that information, but does not include technical details about the database.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/022*) – Awareness of use of images

Asked:

How would a person know that their image has been used as a comparator via the Face Identification Service?

Answer:

Individuals will not be specifically notified when their image is accessed through the Face Identification Service (FIS). This is similar to current law enforcement and security agency practices, where identification information may be obtained by these agencies from other agencies for the purpose of investigations. At present, these agencies would not typically notify those individuals that their information had been obtained in the course of an investigation.

Individuals will however be made aware of the fact that their information may be accessed through the FIS. This will occur at the time that people provide their information for the purpose of obtaining a government identification document that may be accessed through the face matching services.

The Department of Home Affairs is also making information available online about the operation of the face matching services so that the community can understand how their data is used through the services.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/023*) – Authorisation for access

Asked:

What level of authorisation will be required for access to the Face Identification Service? Where is this provided for in the Bill?

Answer:

The Bill restricts the provision of the Face Identification Service (FIS) to certain agencies (listed at subclause 8(2) of the Bill) and for certain activities (the identity and community protection activities set out in subclauses 6(2) to 6(6) of the Bill).

Additional authorisation requirements for use of the FIS will be set out in the Face Matching Services Participation Agreement (Participation Agreement). The Participation Agreement will require user agencies to limit access to the FIS to those employees who have specialist functions and who have a reasonable need to access the service to perform their functions.

The Participation Agreement will also provide that certain types of FIS queries require a user to obtain authorisation from a senior officer. These include queries which:

- are to identify a witness to a crime,
- are for community safety purposes,
- involve a person suspected to be under the age of 18 years; or
- requesting a larger image gallery than the default maximum (of 20 images).

The Agreement will also require that authorising officers must be either a commissioned police officer or another officer of equivalent seniority.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/024*) – Disclosures of information

Asked:

In what circumstances will a disclosure of information under the Identity Data Sharing Service be allowed? What types of information will be allowed to disclosed?

Answer:

The Identity Data Sharing Service (IDSS) will facilitate the transfer of identification information between participating agencies that have a legal basis to share that information. As with all the identity-matching services defined under the Bill, only 'identification information' (as defined at clause 5 of the Bill) will be able to be shared through the IDSS; and the purpose for sharing the information must fall within the identity and community protection activities set out in the Bill.

The Bill itself does not authorise participating agencies to share information through the IDSS (or any of the other identity-matching services). It only provides the Department of Home Affairs with the authorisation it needs to provide the service. All disclosures of information between participating agencies using the IDSS will therefore need to have a legal basis under other legislation, including Commonwealth, state or territory privacy legislation or agency-specific legislation.

An example of this may be where a police force confiscates a large collection of false identification documents, such as passports. The police force could use the IDSS to securely send electronic copies of the false or fraudulently obtained documents to the Department of Foreign Affairs and Trade (DFAT), which manages passport issuing, so that DFAT can take appropriate action (including cancelling the documents). The interoperability hub will provide a secure connection between the two agencies to facilitate this data transfer.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/025*) – Disallowable instruments

Asked:

Would there be any impediments the rule making powers in the Bills so that the powers are exercised as a disallowable instrument in force for 40 days — to be followed by amendments to be brought to Parliament — which is reviewable by the Committee within 15 Parliamentary sitting days?

Answer:

Subject to the views of the Office of Parliamentary Counsel in relation to technical drafting, the Department of Home Affairs does not consider that there would be any policy impediments to this type of arrangement. However, 40 days is a very short time period within which to prepare legislative amendments and have them pass through Parliament – the 2018 Parliamentary sittings calendar contains a number of non-sitting periods of greater than 30 days. The Department considers three months would be a more appropriate period of time for the instrument to remain in force and this time period is consistent with, for example, special security directions contained in Division 7 of Part 4 of the *Aviation Transport Security Act 2004* (the Act) which remain in force for an initial period of three months after which amendments can be made to the Act or associated regulations.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/026*) – Data breaches

Asked:

Have there been any data breaches in relation to the existing Face Verification Service?

Answer:

There have been no data breaches in relation to the use of the Face Verification Service.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 17 August 2018

HOME AFFAIRS PORTFOLIO

(*IMS/027*) – Reporting of security incidents

Asked:

Would there be any impediment on the Department reporting on the statistics only of any security incidents in relation to use of the identity-matching services?

Answer:

It would be feasible for the Department of Home Affairs to report on statistics relating to any security incidents relating to the use of the identity-matching services by various Commonwealth, state and territory agencies. To do so the Department would be reliant on these agencies reporting such incidents to the Department. This will be a requirement of the Face Matching Services Participation Agreement. However, any reporting would best be confined to just the statistics of incidents – requiring the naming of the agency responsible may make some agencies more reluctant to provide this information to the Department.

The Department's participation in the identity-matching services is already subject to the Notifiable Data Breaches scheme established under Part IIIC of the *Privacy Act 1988* (Privacy Act). This includes the Department's operation of the interoperability hub, the Department's immigration and citizenship data holdings and the personal information that it will hold in the National Driver Licence Facial Recognition Solution. Many other Commonwealth agencies are also subject to this scheme, including the Department of Foreign Affairs and Trade in relation to the passports data that it holds and is making available through the face matching services.

Under the Notifiable Data Breaches scheme, agencies are required to report to the Information Commissioner any breaches that fall within the scheme, including unauthorised access to personal information that is likely to result in serious harm to individuals. Due to the nature of the information contained in the databases accessible through the face-matching services – which includes government identification document information and facial images (which are categorised as 'sensitive information' under the Privacy Act) - breaches of these databases are likely to fall within the scheme.

Chapter 9 of the Guide to Privacy Regulation Action published by the Office of the Australian Information Commissioner (OAIC) states that the OAIC will publish statistics in relation to the Notifiable Data Breaches scheme.

The Department considers that reporting statistics of other security incidents relating to the use of the identity-matching may create duplication and/or confusion with reporting under the Notifiable Data Breaches scheme – with potential to equate less serious incidents with the serious data breaches that are covered by the scheme.