
Parliamentary Joint Committee on Intelligence and Security
List of Recommendations

Recommendation 1

5.7 The Committee recommends that the Identity-matching Services Bill 2019 be re-drafted taking into account the following principles:

- the regime should be built around privacy, transparency and subject to robust safeguards,

- the regime should be subject to Parliamentary oversight and reasonable, proportionate and transparent functionality,

- the regime should be one that requires annual reporting on the use of the identity-matching services, and

- the primary legislation should specifically require that there is a Participation Agreement that sets out the obligations of all parties participating in the identity-matching services in detail.

The Identity-matching Services Bill 2019 should be re-drafted taking into account the Committee’s findings in this report. The Committee notes that the findings alone do not set out all of the matters that would bring the Identity-matching Services Bill 2019 into line with the principles outlined above.

Recommendation 2

5.8 The Committee recommends that, following implementation of recommendation one of this report and subsequent re-introduction to the House, the Identity-matching Services Bill 2019 be referred to the Committee for further review.
Recommendation 3

6.21 The Committee recommends that the Australian Passports Amendment (Identity-matching Services) Bill 2019 be amended to ensure that automated decision making can only be used for decisions that produce favourable or neutral outcomes for the subject, and that such decisions would not negatively affect a person’s legal rights or obligations, and would not generate a reason to seek review.

Recommendation 4

6.23 The Committee recommends that, following the implementation of Recommendation 3, the Passports Amendment Bill not proceed until the Committee has completed its review of the revised version of the Identity-matching Services Bill 2019 (as anticipated by Recommendation 2). If, as a consequence of amendments made to the IMS Bill, further amendments are made to the Passports Amendment Bill, the Passports Amendment Bill should, in accordance with Recommendation 2, also be referred to the Committee for further review.
Terms of Reference

On 31 July 2019, the Attorney-General, the Hon Christian Porter MP, wrote to the Committee to refer the provisions of the Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019 to the Committee for inquiry and report.
Members

Chair
Mr Andrew Hastie MP

Deputy Chair
Hon Anthony Byrne MP

Members
Hon Mark Dreyfus QC, MP  Senator the Hon Eric Abetz
Hon Dr Mike Kelly AM, MP  Senator the Hon David Fawcett
Mr Julian Leeser MP  Senator the Hon Kristina Keneally
Mr Tim Wilson MP  Senator Jenny McAllister

Senator Amanda Stoker
Contents

List of Recommendations ........................................................................................................... iii
Terms of Reference .................................................................................................................... v
Members ..................................................................................................................................... vii

The Report

1  Introduction ............................................................................................................................. 1
2  Biometric systems and privacy ............................................................................................ 21
3  Identity-matching services, the interoperability hub and the National Drivers License Recognition Solution ............................................................................................................................... 39
4  Collection, use, protection and disclosure of identification information and reporting and review requirements ......................................................................................................................... 67
5  A workable identity-matching regime .................................................................................. 75
6  Australian Passports Amendment (Identity-matching Services) Bill 2019 93

Appendix A. List of submissions ................................................................................................. 99
Appendix B. List of witnesses appearing at the public hearings .............................................. 103
1. Introduction

The Bills and their referral

1.1 On 31 July 2019, the Hon David Coleman MP, the Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs, introduced the Identity-matching Services Bill 2019 (IMS Bill) into the House of Representatives.

1.2 In his second reading speech, the Minister stated that:

The identity-matching services to be enabled by this bill include a Face Verification Service which will make it easier for documents containing facial images to be safely verified online, making access to government services more secure, accessible and convenient for citizens. This means that, over time, more and more services can be provided completely online, making life easier for everyday Australians.¹

1.3 At the same time, the Minister also introduced the Australian Passports Amendment (Identity-matching Services) Bill 2019 (Passports Amendment Bill) to the House of Representatives.

1.4 In his second reading speech the Minister stated that the Passports Amendment Bill

¹ The Hon David Coleman MP, the Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs, House of Representatives Hansard, 31 July 2019, p. 11.
will provide a clear legal basis for ensuring that the foreign minister is able to
direct the automation of the sharing of passport data for the purposes of
national security.²

1.5 On 31 July 2019, the Attorney-General, the Hon Christian Porter MP, wrote
to the Committee to refer the provisions of both bills for inquiry.

1.6 On 8 August 2019, the Hon Peter Dutton MP, Minister for Home Affairs,
wrote to the Committee and requested that, as far as possible, the
Committee conduct its inquiry in public.

**Context of the inquiry**

1.7 These are re-introduced Bills. The Identity-matching Services Bill 2018 and
the Australian Passports Amendment (Identity-matching services) Bill 2018
lapsed upon this year’s election. At this time the Committee’s review of the
Identity-matching Services Bill 2018 and the Australian Passports
Amendment (Identity-matching services) Bill 2018 (previous inquiry) also
lapsed.

1.8 Pursuant to Clause 8 of Schedule 1 of the *Intelligence Services Act 200*, the
Committee has accepted as evidence to its review of the Identity-matching
Services Bill 2019 and the Australian Passports Amendment (Identity-
matching services) Bill 2019 all evidence, including submissions and
transcripts taken, for the Committee’s review of the Identity-matching
Services Bill 2018 and the Australian Passports Amendment (Identity-
matching services) Bill 2018.

**Conduct of the inquiry**

1.9 The Committee announced the inquiry by media release on 9 August 2019
and invited submissions from interested members of the public by
6 September 2019.

1.10 For its previous inquiry the Committee received 20 submissions and eight
supplementary submissions from industry, government and other
organisations. During this inquiry the Committee received 20 submissions.
A list of submissions received by the Committee is at Appendix A.

---

² The Hon David Coleman MP, the Minister for Immigration, Citizenship, Migrant Services and
1.11 During its previous inquiry the Committee held public hearings on 3 May 2018 and 17 August 2018. The Committee also received a private briefing on 17 August 2018. A list of hearings and witnesses who appeared before the Committee is included at Appendix B.

1.12 Copies of submissions received and transcripts of public hearings can be accessed on the Committee’s website at: [http://www.aph.gov.au/pjcis](http://www.aph.gov.au/pjcis). Links to the Bills and Explanatory Memorandums are also available on the Committee’s website.

**Report structure**

1.13 The report consists of five chapters:

- This chapter sets out the context and conduct of the inquiry, provides an outline of the Bills and examines the rationale for the Bills,
- Chapter 2 examines biometric systems and considers the privacy and other human rights implications of the Bills,
- Chapter 3 examines the identity-matching services, the interoperability hub and the National Driver Licence Facial Recognition Solution (NDLFRS – referred to in this report as Driver Recognition Solution),
- Chapter 4 considers the collection, use, protection and disclosure of identification information, and reporting and review requirements,
- Chapter 5 contains the Committee’s principles and findings in relation to the IMS Bill, and
- Chapter 6 examines the Passports Amendment Bill and sets out the Committee’s concluding comments.

**Outline of the bills**

**Identity-matching Services Bill 2019**

**Background on the Bill’s development**

1.14 The IMS Bill seeks to facilitate the secure, automated and accountable exchange of identity information between the Commonwealth and state and territory governments pursuant to the objectives of the *Intergovernmental Agreement on Identity Matching Services* (IGA), agreed by the Council of Australian Governments (COAG) in October 2017.  

---

3 Identity-matching Services Bill 2019 (IMS Bill), Explanatory Memorandum, p. 2.
1.15 It implements goals set out in the National Identity Security Strategy and the National Facial Biometric Matching Capability and provides for identity-matching services as additions to the existing Document Verification System. The Identity Strategy, the Facial Matching Capability, the Document Verification System and the IGA are explained in more detail below.

**Overview**

1.16 Broadly, the IMS Bill seeks to establish a range of services to identify, recognise or verify a facial image. In addition, it proposes systems for the collation, access, use, sharing and disclosure of this type of data.

1.17 The IMS Bill authorises the Department of Home Affairs to create and maintain facilities for the sharing of facial images and other identity information between government agencies, and in some cases, non-government entities. Further, the Bill authorises the Department to develop, operate and maintain two centralised facilities for the provision of identity-matching services:

- an **interoperability hub**, intended to operate as a router through which participating government agencies and non-government entities can request and transmit information as part of an identity-matching service, and

- the **National Driver Licence Facial Recognition Solution** (referred to in the Bill as the NDLFRS), a federated database of information contained in government identity documents such as driver licences.

1.18 The IMS Bill does not authorise certain agencies to use identity-matching services. Rather, entities seeking access will need a legal basis for collecting and disclosing personal information and must meet access requirements set out in the IGA.

1.19 The IMS Bill consists of five parts, which are outlined in more detail in the following section.

**Part 1 – Preliminary and Definitions**

1.20 Part 1 of the IMS Bill consists of two divisions. Division 1 sets out the preliminaries, such as short title and commencement.

1.21 Division 2 is split into two subdivisions. Subdivision A includes general definitions used elsewhere in the Bill, including the definitions of ‘identification information’ and ‘identity or community protection activity’.
Subdivision B includes definitions relating to identity-matching services. It defines an ‘identity-matching service’ as any of the following:

- Face Identification Service,
- Facial Recognition Analysis Utility Service,
- Face Verification Service,
- Identity Data Sharing Service, and
- One Person One Licence Service.\(^4\)

1.22 The IMS Bill also provides that additional services may be prescribed in rules.\(^5\) Each of the above-listed services will be accessed through the interoperability hub or the National Driver Licence Facial Recognition Solution, and are defined in Table 1.1 below.

Table 1.1  List of identity-matching services

<table>
<thead>
<tr>
<th>Service</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Face Identification Service  
(referred to in the IMS Bill as the FIS)     | This service will search facial images on a one-to-many basis or help determine the identity of an unknown person, or detect instances where a person may hold multiple fraudulent identities.\(^6\) |
| Facial Recognition Analysis Utility Service  
(referred to in the IMS Bill as the FRAUS)  
(referred to in this report as the Facial Recognition Service) | This service will allow state and territory agencies to assess the accuracy and quality of their data holdings.\(^7\) |
| Face Verification Service  
(referred to in the IMS Bill as the FVS)     | This service will enable a user to verify a specific person’s identity by using a facial image and associated biographic details of a |

\(^4\) IMS Bill, section 7.  
\(^5\) IMS Bill, section 7.  
\(^6\) IMS Bill, section 8.  
\(^7\) IMS Bill, section 9.
A person to be compared on a one-to-one basis against an image held on a specific government record for that same individual. Non-government entities and local governments may seek access to this service.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Person One Licence Service</td>
<td>This service will allow state and territory agencies to detect instances where a person may hold multiple driver licences across jurisdictions.</td>
</tr>
<tr>
<td>Identity Data Sharing Service</td>
<td>Not technically an identity-matching service but this service will allow for the sharing of biometric identity information between Commonwealth, state and territory agencies.</td>
</tr>
</tbody>
</table>


Part 2 – Developing and operating the interoperability hub and National Driver Licence Facial Recognition Solution

1.23 Part 2 provides for the Secretary of the Department of Home Affairs to develop and operate the ‘interoperability hub’ and the National Driver Licence Facial Recognition Solution.

1.24 The ‘interoperability hub’ is a facility for relaying electronic communications between bodies and persons for the purposes of requesting and providing identity-matching services.

8 IMS Bill, section 10.
9 IMS Bill, section 12.
10 IMS Bill, section 11.
11 The IMS Bill is drafted referring to ‘the Secretary’ and ‘the Minister’. Currently the Department responsible for the Bill is the Department of Home Affairs and the responsible Minister is the Hon Peter Dutton MP, Minister for Home Affairs.
The National Driver Licence Facial Recognition Solution will include a database of identification information from state and territory authorities and will make driver licence facial images available through an identity-matching service.\(^\text{13}\)

**Part 3 – Authorising collection, use and disclosure of identification information**

1.26 Part 3 consists of three divisions. Division 1 contains a simplified outline of the Part.

1.27 Division 2 deals with the collection, use and disclosure of identification information by the Department of Home Affairs. The Department may collect, use or disclose identification information through the interoperability hub or the National Driver Licence Facial Recognition Solution for any of the following purposes:

- providing or developing an identity-matching service for the purpose of an ‘identity or community protection activity’,\(^\text{14}\)
- protecting an assumed identity acquired under Part 1AC of the *Crimes Act 1914* or the real identity of a person who has acquired an assumed identity,\(^\text{15}\) or
- protecting an identity that has been provided under a witness identity law or scheme.\(^\text{16}\)

1.28 An activity will be an ‘identity or community protection activity’ if it relates to one of the following:

- preventing and detecting identity fraud,
- law enforcement activities,
- national security activities,
- protective security activities,
- community safety activities,
- road safety activities, or
- verifying identity.\(^\text{17}\)

---

\(^{12}\) IMS Bill, section 14.

\(^{13}\) IMS Bill, section 15.

\(^{14}\) IMS Bill, sections 17(2)(a)-(c), 18.

\(^{15}\) IMS Bill, sections 17(2)(d), 18.

\(^{16}\) IMS Bill, sections 17(2)(e), 18.
Division 3 deals with the disclosure of identification information by state and territory authorities to the Department. The Division provides that, if a law of the state or territory limits an authority’s disclosure of identification information and an exemption in relation to a law of the Commonwealth applies, that authority may disclose that information to the Department via electronic communication.\footnote{IMS Bill, section 19.}

**Part 4 – Protection of information**

Part 4 sets out provisions around the protection of information and consists of two divisions. Division 1 contains a simplified outline of the Part.

Division 2 establishes an offence where an ‘entrusted person’\footnote{An ‘entrusted person’ is, in short, an employee or contractor of the Department of Home Affairs. IMS Bill, section 21(4).} obtains ‘protected information’\footnote{‘Protected information’ includes information communicated to or from the interoperability hub or the National Driver Licence Facial Recognition Solution, or information that otherwise relates to the operation of the interoperability hub or the National Driver Licence Facial Recognition Solution. IMS Bill, section 21(4).} and makes a record of, or discloses, it to another person. The offence is punishable by imprisonment for two years.

The IMS Bill provides for an exception to the offence where the conduct is authorised by a law of the Commonwealth or of a state or territory.\footnote{IMS Bill, section 21.}

Division 3 provides for authorised recording and disclosure of protected information by entrusted persons. An entrusted person may make a record of, or disclose, protected information if they do so with the consent of the person\footnote{IMS Bill, section 25.} or for the purposes of:

---

\footnote{IMS Bill, section 6.}
\footnote{IMS Bill, section 19.}
\footnote{IMS Bill, section 21.}
- the IMS Bill,\textsuperscript{23}
- lessening or preventing a threat to life or health,\textsuperscript{24} and
- a corruption issue.\textsuperscript{25}

**Part 5 – Delegation of Secretary’s powers and functions, annual reporting and review of operation of the Act**

1.34 Part 5 allows for the Secretary, in writing, to delegate his or her functions or powers proposed by the IMS Bill to an SES employee or acting SES employee of their Department.

1.35 Proposed section 28 of the IMS Bill requires the Secretary to give the Minister an annual report, for presentation in Parliament. The report is required to provide detail on statistics relating to all requests in the financial year from:

- authorities of the Commonwealth (except the Australian Security Intelligence Organisation) or of a State or Territory, for a Face Identification Service, Face Verification Service or One Licence Service, and
- non-government entities for a Face Verification Service.

1.36 In addition, the annual report must include information on each authority of the Commonwealth (except the Australian Security Intelligence Organisation), and each authority of a State or Territory (including a local government authority), that used an Identity Data Sharing Service to disclose or collect identification information in the financial year.

1.37 Proposed section 29 provides for a review of the operation of the Act and provision of identity-matching services to be started within five years of the commencement of the Act. Proposed section 30 provides for a general rule making power for the Minister.

1.38

\textsuperscript{23} IMS Bill, section 22.
\textsuperscript{24} IMS Bill, section 23.
\textsuperscript{25} IMS Bill, section 24.
Australian Passports Amendment (Identity-matching Services Bill) 2019

1.39 The Passports Amendment Bill authorises the Department of Foreign Affairs and Trade to disclose information in order to participate in identity-matching services and provides for computerised decision-making. It consists of one schedule that inserts two new sections into the Australian Passports Act 2005.

1.40 Proposed section 46(da) authorises the Minister for Foreign Affairs to disclose personal Australian travel document data for the purpose of participating in a service specified in the Minister’s determination, to share or match information relating to the identity of a person. In practice this will allow the Minister for Foreign Affairs to make a determination allowing disclosure of information for the identity-matching services as provided for in the IMS Bill.

1.41 Proposed section 56A will incorporate scope for the Minister for Foreign Affairs to automate decisions under the Australian Passports Act 2005.

Rationale for the bills

Identity-matching Services Bill 2019

1.42 In its submission, the Department of Home Affairs cited the serious impact of identity crime as a driver for the measures proposed in the Bill:

   Identity crime causes substantial harm to the economy and individuals each year. The Identity Crime and Misuse in Australia Report 2016 prepared by the Attorney-General’s Department, in conjunction with the Australian Institute of Criminology, indicated that identity crime impacts around 1 in 20 Australians every year (and around 1 in 5 Australians throughout their lifetime), with an estimated annual cost of over $2.2 billion.\textsuperscript{26}

1.43 Since at least 2007, there have been a range of Commonwealth, state and territory government agreements, strategies and services to address issues of identity crime. The IMS Bill proposes a formal operational framework for national identity matching services.

\textsuperscript{26} Department of Home Affairs, \textit{Submission 12}, p. 4.
National Identity Security Strategy

1.44 In 2007, heads of COAG signed an Intergovernmental Agreement on an Identity Security Strategy (the Identity Strategy), aimed at combatting identity theft and the fraudulent use of stolen and assumed identities. The parties agreed to strengthen government processes and standards for identifying (and verifying the identity of) persons, including through enhancing the interoperability of biometric security measures.

1.45 The Identity Strategy was revised in 2012. One goal of the revised Strategy was the development of a National Biometric Interoperability Framework, setting out guiding principles for ensuring a consistent approach to the collection, use, disclosure and management of biometrics. The Framework is intended to work within existing legislation, and improve the interoperability of biometric systems across jurisdictions.

Document Verification Service

1.46 Arising out of the Identity Strategy was the Document Verification Service which has been operational in the public sector since 2009. The Document Verification Service enables the comparison of details on an identity document with records held by the issuing authority, to verify that the details are still valid and the document is legitimate.

1.47 In a similar way to the identity-matching services provided for in the IMS Bill, data is not stored on the Document Verification Service itself. Instead, requests to verify a person’s identifying information are encrypted and sent

---


through a secure ‘Document Verification Service hub’ to the issuing authority.\(^{33}\) In most circumstances, the person must provide express consent for their personal information to be used in this way.\(^{34}\)

1.48 The Explanatory Memorandum to the IMS Bill identifies shortcomings in the capacity of the Document Verification Service to detect all forms of identity crime:

[the Service] helps to prevent the use of fake identities (false names, dates of birth etc) by detecting when a document does not match a record held by the issuing authority. However, this has incentivised criminals to steal genuine identities and use them for criminal purposes, rather than create entirely false identities. Organised crime groups in particular are developing increasingly sophisticated methods for replicating genuine identification documents with fake photographs, using the same technologies issued by the document-issuing agency. These documents are not detected by the DVS because the biographical details are genuine.\(^{35}\)

**National Facial Biometric Matching Capability**

1.49 In October 2014, a meeting of COAG’s then-Law, Crime and Community Safety Council\(^ {36}\) noted the Commonwealth’s plans to establish a National Facial Biometric Matching Capability (Capability). This Capability would provide a mechanism for the cross-jurisdictional sharing of existing information collected by agencies.\(^ {37}\)

1.50 In September 2015, the then Minister for Justice, the Hon Michael Keenan MP, announced that the Commonwealth was spending $18.5 million to develop the Capability. The announcement noted that the Capability would initially involve ‘one-to-one’ image-based verification between

---


35 IMS Bill, Explanatory Memorandum, p. 46.

36 The Law, Crime and Community Safety Council (LCCSC) was made up of ministers with responsibility for law and justice, police and emergency management in each Australian state and territory, as well as two ministers from the Australian and New Zealand Governments. Following a COAG review in 2016–17, the LCCSC was replaced with separate councils for Attorneys-General and Ministers for Police and Emergency Management.

Commonwealth agencies, with more agencies to join over time. It would then be further developed to allow ‘one-to-many’ identification matching, enabling law enforcement and security agencies to match the photograph of an unknown person against the photos in government records, to establish the person’s identity.\textsuperscript{38} The then Minister for Justice stated

\begin{quote}
the new capability will allow agencies to match a person’s photograph against an image on one of their government records. This will help prevent more insidious forms of identity fraud – where criminals create fake documents using their own photos, with personal information stolen from innocent victims. It will also assist victims more easily restore their compromised identities.\textsuperscript{39}
\end{quote}

1.51 The Face Verification Service commenced operation in November 2016, enabling the Department of Foreign Affairs and Trade and the Australian Federal Police to access citizenship images held by the Immigration Department. At the time of the launch it was announced that other types of images such as visa, passport and driver licence photos would be added over time, and that access would subsequently be expanded to other government agencies.\textsuperscript{40}

\textbf{Intergovernmental Agreement on Identity Matching Services}

1.52 The Intergovernmental Agreement on Identity Matching Services (IGA) was agreed by COAG in October 2017 and signed by the Commonwealth and all states and territories

1.53 Clause 1.2 of the IGA provides that the parties agree to promote the sharing and matching of identity information for the purposes of:

\begin{itemize}
  \item preventing identity crime,
  \item general law enforcement,
  \item national security,
  \item protective security,
  \item community safety,
\end{itemize}

\textsuperscript{38} M Keenan (Minister for Justice), \textit{New $18.5 million biometrics tool to put a face to crime}, media release, 9 September 2015.

\textsuperscript{39} M Keenan (Minister for Justice), \textit{New $18.5 million biometrics tool to put a face to crime}, media release, 9 September 2015.

\textsuperscript{40} M Keenan (Minister for Justice), \textit{New face verification service to tackle identity crime}, media release, 16 November 2016.
- road safety, and
- identity verification.

1.54 However, the Australia Capital Territory included a variation stating that it would only allow access to its data for the purposes of the Face Verification Service and would not participate in the One Licence Service. Limited access to data via the Face Identification Service would be provided where this was for the purposes of national security and community safety.41

1.55 South Australia also included a variation providing that it would accept the IGA subject to its Public Sector (Data Sharing) Act 2016 authorising the collection, use and disclosure of facial images and related identity information.

1.56 The parties to the IGA agreed that the identity-matching services should be developed and operated in accordance with the principles around privacy, security, data access, data quality, identity resolution decisions resting with Requesting Agencies, a non-evidentiary system, the protection of legally assumed identities and robust accountability.42

Participation Agreements, the Coordination Group and Access Policies

1.57 The IGA provides for a Face Matching Services Participation Agreement (Participation Agreement) which will be a legal agreement between all agencies participating in the identity-matching services. The Participation Agreement will set out the respective roles, rights and obligations of all agencies in relation to their participation in, access to and use of the identity-matching services.43

1.58 The Participation Agreement in relation to the identity-matching services has not commenced and no further information on any Participation Agreements was provided to the Committee.

1.59 The IGA also references the existing National Identity Security Coordination Group (Coordination Group) which comprises representatives from the Commonwealth, States and Territories, and works to implement the Identity Strategy. The Coordination Group will approve ‘access policies’ which are a

---

41 In relation to identity matching the IGA refers to a ‘system’ whilst the IMS Bill refers to a ‘service’.

42 Council of Australian Governments (COAG), Intergovernmental Agreement on Identity Matching Services, 5 October 2017, p. 6.

43 COAG, Intergovernmental Agreement on Identity Matching Services, 5 October 2017, p. 7.
documented set of requirements that an entity must comply with in order to access identity-matching services. Approved access policies for the FVS and the FIS are available on the Australian Government ID Match webpage which has been established specifically for providing information about the Identity Matching Services.

1.60 The Access Policy for the FVS was issued in June 2017 and provides an example of the criteria an agency must meet in order to participate in identity-matching services. In order to gain access to the FVS, an agency must:

- provide a statement referencing legislation that provides the legal basis for using and/or disclosing identity information via the Face Verification Service,
- undertake or contribute to a privacy impact assessment to account for every information flow which occurs through the Face Verification Service, to which the agency is a party (unless the agency’s use of the Face Verification Service is exempt from the relevant Commonwealth, state or territory privacy laws),
- enter into an Interagency Data Sharing Arrangement with each agency with which it intends to share information via the Face Verification Service,
- maintain a register of Nominated Users who are authorised to submit queries via the Face Verification Service, ensure the users undertake training in security awareness and privacy obligations, and ensure that any IT systems connected with the hub receive and maintain appropriate security accreditation,
- have an independent audit conducted of all its data sharing via the Face Verification Service at least once every financial year, and
- enter into a memorandum of understanding with the Department of Home Affairs in relation to the services through the interoperability hub.

---


The Access Policy for the FIS has similar access criteria. The Department of Home Affairs is responsible for reviewing each Interagency Data Sharing Arrangement to ensure consistency with the Access Policy, and for reviewing audit and compliance reports.

**State and territory legislation**

The IGA does not provide agencies with the legal authority to share information—it is intended that this authorisation is to come from the laws of each state and territory. Part 8 of the IGA provides that each jurisdiction will preserve or introduce legislation as necessary, to support the collection, use and disclosure of facial images and related identity information between the parties.

In Queensland the *Police and Other Legislation (Identity and Biometric Capability) Amendment Act 2018* was enacted on 16 March 2018.

Tasmania has amended its driver licensing regulations to authorise the disclosure of protected information for the purposes of identity-matching services. South Australia has indicated that the *Public Sector (Data Sharing) Act 2016* (SA) meets its legislative obligations for the purposes of the agreement, suggesting that further legislation may not be required.

**Australian Passports Amendment (Identity-matching Services) Bill 2019**

The Explanatory Memorandum to the Passports Amendment Bill states that the Bill amends the *Australian Passports Act 2005* (Passports Act) to provide a legal basis for ensuring that the Minister is able to make Australian travel document data available for all the purposes of, and by the automated means intrinsic to,

---


the identity-matching services to which the Commonwealth and the States and Territories agreed in the *Intergovernmental Agreement on Identity Matching Services* (IGA), signed at a meeting of the Council of Australian Governments on 5 October 2017.\(^51\)

**General view on the objectives of the Bills**

**Identity-matching Services Bill 2019**

1.67 Those submitters who addressed the underlying objectives and rationale for the IMS Bill offered broad support. However, this support did not always extend to the implementation mechanisms proposed in the Bill.

1.68 The Victorian Government supported the use of the IMS Bill ‘to prevent identity crime and to assist general law enforcement, national and protective security, community and road safety, and identity verification’.\(^52\)

1.69 Optus and the Australian Mobile Telecommunications Association both provided support for the key provisions of the Bill. The telecommunications industry representatives submitted that the Bill would improve public confidence in identity validation and assist in preventing identity theft and fraud.\(^53\)

1.70 The Office of the Information Commissioner (Queensland) also offered in-principle support to the objectives of the IMS bill and the ‘nation-wide regime it will help facilitate’.\(^54\)

1.71 Similarly, Australian Lawyers for Human Rights agreed with the broad rationale for the IMS Bill stating that they did not ‘disagree with the aim of allowing identity-matching services to be used by government’ but still had concerns that sufficient safeguards had not been adopted in the IMS Bill. They stated that information ‘obtained through or used by these government services could be made available for commercial purposes’.\(^55\)

\(^{51}\) *Australian Passports Amendment (Identity-matching Services) Bill 2019 (Passports Amendment Bill), Explanatory Memorandum*, p. 2.

\(^{52}\) *Victorian Government, Submission 14*, p. 1.

\(^{53}\) *Australian Mobile Telecommunications Association, Submission 26*, p. 2 and *Optus, Submission 28*, p. 2.

\(^{54}\) *Office of the Information Commissioner (Queensland), Submission 3*, p. 2.

Likewise the Office of the Victorian Information Commissioner offered in-principle support for the ‘use of the identity-matching services in the context of national security’ however the Office had concerns that risk will largely be managed via agreements between the parties rather than through the legislation itself. The Office questioned the enforceability of these agreements and suggested that the ‘ability for fundamental controls to be amended without parliamentary oversight may also be problematic’.  

The Human Rights Law Centre also welcomed the approach of ‘providing a legislative framework for the retention, use and sharing of facial images and other biometric data’.  

The Office of the Australian Information Commissioner stated that they support ‘measures that aim to address identity-related crime, and enable law enforcement bodies to cooperate to achieve this objective’, but noted that the IMS Bill ‘requires further consideration to better ensure that any adverse effects of the proposed enactment on the privacy of individuals are minimised’.  

The Human Rights Law Centre stated that:

Much of the justification for the Bill is focused on the need to address identity theft and serious crime, like terrorism. It’s very easy to see how the bill will help to address these issues, which will advance human rights. But the very broad drafting of the bill enables uses far beyond that, which creates serious risks to other human rights like privacy, freedom of association, freedom of expression and assembly, and freedom from discrimination.  


60 Mr Hugh de Kretser, Executive Director, Human Rights Law Centre, *Committee Hansard*, Canberra, 17 August 2018, p. 1.
Australian Passports Amendment (Identity-matching Services) Bill 2019

1.76 Most submitters focussed their evidence on the IMS Bill. Where submitters did comment on the Passports Amendment Bill, they focussed on matters of detail that are dealt with in Chapter 6 of this report.

Committee comment

1.77 The Committee expresses its support for the rationale behind the IMS Bill and the Passports Amendment Bill, and national cooperative measures to curb identity crime and its links to national security threats.

1.78 In relation to the IMS Bill in particular, the Committee notes that much of the ‘architecture’ of the identity-matching services is left to Access and Participation Agreements or the practices of data holding agencies. This lack of detail in the IMS Bill has prompted many of the concerns raised by submitters to the Committee’s inquiry. Chief among these concerns was privacy.

1.79 The following chapter examines biometric systems and considers the privacy and other human rights implications of the bills.
2. Biometric systems and privacy

2.1 This chapter discusses the central issue raised in evidence to the Committee’s review of the two bills: privacy concerns with the sharing, use, security and reliability of biometric data.

2.2 First, the chapter outlines biometrics and biometric identification, and presents stakeholder concerns about the security, use and reliability of this type of information. Second, the chapter examines the privacy concerns raised in evidence including the source of the right to privacy (under international law and the Australian Privacy Principles) and the extent to which those rights are maintained in the Intergovernmental Agreement on Identity Matching Services (IGA) and the IMS Bill.

2.3 Finally, the chapter discusses other human rights concerns raised by stakeholders: freedom of movement, the right to non-discrimination, and the right to a fair trial.

2.4 The Committee’s comment on each of these concerns, and its recommendations for amendment, appear at the end of the chapter.

Biometrics and biometric identification

2.5 The Biometrics Institute defines biometrics as covering a variety of technologies in which unique attributes of people are used for identification.

---

1 The Biometrics Institute was founded in July 2001 responding to an industry need for an independent and impartial international forum for the sharing of knowledge and information.
and authentication. This includes a person’s fingerprint, iris print, hand, face, voice, gait or signature, which can be used to validate the identity of individuals seeking to control access to computers, airlines, databases and other areas which may need to be restricted.\textsuperscript{2}

2.6 The Biometrics Institute cites the following as different types of biometrics:

- DNA matching,
- ear shape,
- eyes – iris recognition,
- eyes – retina recognition,
- face recognition,
- fingerprint recognition,
- finger geometry recognition,
- gait,
- hand geometry recognition,
- odour,
- signature recognition,
- typing recognition,
- vein recognition,
- voice/speaker recognition,
- voice/speaker verification/authentication, and
- voice – speaker identification.\textsuperscript{3}

**Security, use and reliability concerns**

2.7 While the Explanatory Memorandum to the IMS Bill states that ‘using facial biometrics can make government and private sector services more accessible and convenient to citizens’,\textsuperscript{4} a number of submitters raised concerns regarding the use of biometric technologies.

2.8 For example, Electronic Frontiers Australia (EFA) pointed to a risk that the security of biometric data contained in the interoperability hub could be compromised, with unintended consequences. EFA stated that

---


\textsuperscript{3} Biometrics Institute, *Types of Biometrics*, see <https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/> viewed 10 October 2019.

\textsuperscript{4} IMS Bill, Explanatory Memorandum, p. 4.
the collection, use and disclosure of personal and sensitive information for the purpose of “protecting Australians against identity theft” may correspondingly become the vehicle by which Australian’s identities are compromised.  

2.9 The Australian Human Rights Commission (AHRC) questioned the security and accuracy of biometrics. The AHRC cautioned that, because biometrics are based on what are considered unique characteristics, ‘there is a risk that biometric identification may be perceived to be more accurate than may be the case’. In addition, the Commission also argued that the use of biometrics creates new risks and may increase the risk of identity fraud and theft.

2.10 In regards to facial recognition technology, the Commission raised privacy concerns and the need for strict controls around use of this technology:

The intrusions into citizens’ privacy that are enabled by facial recognition technology are real, and they are profound. It has been said that the technology may herald ‘the end of anonymity’. For that reason, particular care needs to be taken to ensure that the use of biometric technologies, including facial recognition technologies, is strictly controlled.

2.11 The Human Rights Law Centre (HRLC) had specific concerns about the accuracy of facial recognition technologies. In particular, the HRLC referred to false positives and false negatives. False positives occur where a person is wrongly identified. This can lead to them being the subject of further investigation or denial of essential services, without justification. False negatives occur when someone is not identified as being who they are. The HRLC considered this of particular concern ‘in the visa or border control context, or in the context of the provision of essential services’. According to the HRLC such misidentification risks ‘eroding trust in government agencies, law enforcement and security agencies’.

2.12 The Department of Home Affairs acknowledged accuracy and bias concerns and stated that it had been very careful in its trials to use a broad

---

5 Electronic Frontiers Australia, Submission 40, p. (8).
10 Human Rights Law Centre, Submission 16, p. 16.
cross-section of the demographic mix of Australia.\textsuperscript{11} In addition the Department explained that it is encouraging agencies that are prescribed to use the identity-matching services to only allow specialist officers with recognised aptitude in facial recognition — supplemented by training — access to the services.\textsuperscript{12}

2.13 The Law Council of Australia also commented on the need for controls and oversight with regards to the use of biometric data, stating that ‘oversight of the retention, collection and use of biometric information is a substantial role’ and suggested the need for a specific oversight authority. Dr Marcus Smith noted that Australia has ‘no independent, specific oversight mechanisms exist to oversee or regulate the collection, retention and use of biometric information’.\textsuperscript{13}

2.14 The Law Council of Australia referenced the United Kingdom’s Commissioner for the Retention and Use of Biometric Material (the UK Biometrics Commissioner) and suggested that consideration be given to establishing a similar commission in Australia.\textsuperscript{14} The joint councils for civil liberties, Future Wise and the Australian Privacy Foundation echoed this recommendation.\textsuperscript{15}

2.15 The UK Biometrics Commissioner was established by the \textit{Protection of Freedoms Act 2012} (UK). The statute introduced a new regime to govern the retention and use by the police of DNA samples, profiles and fingerprints.\textsuperscript{16} The Commissioner is independent of government, and their role is to:

- keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints,

\begin{itemize}
\item Mr Andrew Rice, Assistant Secretary, Identity Security Branch, Department of Home Affairs, \textit{Committee Hansard}, Canberra, 17 August 2018, p. 22.
\item Mr Andrew Rice, Assistant Secretary, Identity Security Branch, Department of Home Affairs, \textit{Committee Hansard}, Canberra, 17 August 2018, p. 23.
\item Dr Marcus Smith, \textit{Submission 17}, p. 4.
\item Law Council of Australia, \textit{Submission 8}, p. 8.
\item Future Wise Australian Privacy Foundation, \textit{Submission 1}, p. 3. This view is shared by the joint councils for civil liberties, \textit{Submission 9}, p. 3.
\end{itemize}
• decide applications by the police to retain DNA profiles and fingerprints (under section 63G of the Police and Criminal Evidence Act 1984 (UK)),
• review national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints, and
• provide reports to the Home Secretary about the carrying out of his or her functions.\textsuperscript{17}

2.16 Dr Smith endorsed the UK Biometrics Commissioner model recommending additional powers in relation to biometric facial images to accommodate for the Australian context. Dr Smith commented that this expanded commissioner role would provide appropriate independent oversight of the developments proposed by these bills, and more broadly. It would be an important step towards ensuring that there is a reasonable and proportionate balance between the need to use available new technology to protect the community from harm, and maintain appropriate standards regarding individual rights.\textsuperscript{18}

2.17 The Department of Home Affairs did not support the creation of a biometrics commissioner to oversight the security and use of biometrics in Australia. While acknowledging that ‘the decision about whether to establish such an office would be a matter for government’, the Department argued that the IMS 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’.\textsuperscript{19}

2.18 Further, the Department maintained that existing oversight is adequate and sufficient, stating that ‘agencies participating in the identity-matching services will continue to be subject to existing oversight arrangements that apply to their activities or functions’.\textsuperscript{20}

\textsuperscript{17} GOV.UK, Office of the Biometrics Commissioner, About Us, see <https://www.gov.uk/government/organisations/biometrics-commissioner/about> viewed 10 October 2019.

\textsuperscript{18} Dr Marcus Smith, Submission 17, p. 5.

\textsuperscript{19} Department of Home Affairs, Submission 12.1, p. 9.

\textsuperscript{20} Department of Home Affairs, Submission 12.1, p. 9.
Privacy concerns

2.19 The majority of submitters to the inquiry raised concerns around privacy. These ranged from broad principle based objections to specific privacy concerns about proposed sections of the bills, particularly the IMS Bill.

2.20 For example, the AHRC noted the range of privacy concerns, stating that ‘biometric systems limit the privacy of individuals in a number of ways’.21 These include that:

- the collection, retention and disclosure of biometric information limits a person’s informational privacy,
- biometric systems will return false positives and release private information about parties who are not subject of the identification request,
- sensitive information may be able to be extracted or inferred from biometric identifiers, and
- biometric systems may facilitate privacy-limiting measures including the collection and collation of large amounts of other information about the individual, as well as the surveillance and tracking of the individual.22

2.21 These concerns were also evident in a number of submissions received from individuals who expressed concern about their right to privacy in the use of facial recognition technology. Some individuals stated that the new capability would be a ‘massive privacy overreach’ and a ‘direct violation of our right to privacy’.23

2.22 The Department of Home Affairs submission stated that the IMS Bill does not seek to provide a ‘blanket exemption to privacy legislation for organisations participating in the identity-matching services’. Agencies making data available through the services, and those organisations seeking to access data through the services, will be subject to legislative privacy protections and information-sharing restrictions that already apply to them and will need to have regard to these when participating in the identity-matching services.24

21 Australian Human Rights Commission, Submission 11, p. 11.
22 Australian Human Rights Commission, Submission 11, p. 11.
24 Department of Home Affairs, Submission 12, p. 5.
International privacy obligations and protections are set out in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), and Australia’s domestic privacy protection regime is set out in the Australian Privacy Principles (APPs) which are contained in Schedule 1 of the Privacy Act 1988. The following sections discuss existing privacy protections and submitter concerns around the efficacy of such protections.

**Right to privacy under international law**

2.24 Article 17 of the ICCPR prohibits arbitrary or unlawful interference with a person’s privacy, family, home or correspondence and unlawful attacks on a person’s honour or reputation. It also provides that everyone has the right to the protection of the law against such interference or attacks.

2.25 The right to privacy articulated in Article 17 of the ICCPR may be subject to permissible limitations that are authorised by law, are not arbitrary, pursue a legitimate objective, are necessary to achieve that objective, and are a proportionate means of achieving it. An interference with the right will not be arbitrary where the interference is consistent with the provisions, aims and objectives of the ICCPR and, is reasonable in the particular circumstances.

2.26 The United Nations Human Rights Committee (the UNHRC) has interpreted ‘reasonableness’ in this context to mean that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.25

2.27 The Statement of Compatibility with Human Rights (Statement) for both the IMS Bill and the Passports Amendment Bill accept that they engage and limit the right to privacy, and provide detailed discussion around this issue. The Statement for the IMS Bill concludes that the provisions they enact are intended to pursue legitimate objectives, are reasonable and necessary to achieve those objectives, and have been designed to ensure that their privacy implications are proportionate to the need for those services for specific activities.26

The Statement for the Passports Amendment Bill comes to a similar conclusion.27

---


26 IMS Bill, Explanatory Memorandum, p. 44.

27 Passports Amendment Bill, Explanatory Memorandum, pp. 4-6.
Stakeholder concerns

2.28 Although many submitters agreed with the objectives of the Bills, they did not agree that the proposed legislative response was proportionate. In a joint submission, Future Wise and Australian Privacy Foundation expressed strong concerns around the privacy intrusions and stated that the IMS Bill should not be passed as it ‘fails to represent a legitimate or proportionate response to the challenges articulated in the Explanatory Memorandum’.28

2.29 Similarly, the AHRC strongly argued against the proportionality of the response and the breadth of use and purpose proposed. The AHRC stated that some of the purposes for which identity-matching services may be used ‘do not appear to be of sufficient weight to justify potentially significant limitations on privacy’. Further, it stated that others ‘are so broadly defined that they might be interpreted to allow law enforcement bodies and intelligence agencies to use the services to collect information without limitation’.29

2.30 Likewise, Australian Lawyers for Human Rights (ALHR) noted that, where human rights are impinged upon, the response must be proportionate and relevant to the harm sought to be addressed. Accordingly they stated their concern that ‘the Bills do not strike the right balance’.30

Parliamentary Joint Committee on Human Rights’ report

2.31 The Parliamentary Joint Committee on Human Rights (Human Rights Committee) reviewed and reported on the bills in two separate reports. The initial report, tabled in March 2018 requested that the Minister for Home Affairs and the Minister for Foreign Affairs advise that Committee as to whether the limitations on the right to privacy are reasonable and proportionate to the measures to achieve the stated objectives in both bills.31

2.32 The Parliamentary Joint Committee on Human Rights’ second and final report on the bills, tabled in June 2018, presented the Ministers’ advice on reasonable and proportional limitations.32 The advice from the Minister for

28 Future Wise and Australian Privacy Foundation, Submission 1, p. 1
30 Australian Lawyers for Human Rights, Submission 2, p. 11.
Home Affairs provided some assurances, however, that Committee expressed ongoing concern that the IMS Bill may ‘be a risk of incompatibility with the right to privacy where the [interoperability hub] facilitates the sharing of information’.  

2.33 The report also identified that the Face Matching Services Participation Agreement—as foreshadowed in the IGA—was considered a central safeguard to the right to privacy. The Committee noted that it did not have access to the Participation Agreement, and accordingly, noted that it was difficult to conclude whether it will ‘provide an adequate and effective safeguard’ to the privacy concerns raised by the IMS Bill.  

The IGA and the Participation Agreement are examined later in this chapter.

2.34 The Committee’s report concluded that the authorisation for an agency to collect, use, share or retain facial images or biographic information may not sufficiently circumscribed so as to satisfy the proportionality and reasonableness test under international law.

2.35 The Human Rights Committee reached a similar conclusion in its consideration of the Passports Amendment Bill following receipt of advice from the Minister for Foreign Affairs.

**Right to privacy under domestic law**

2.36 Schedule 1 of the *Privacy Act 1988* sets out the Australian Privacy Principles (APPs) which apply to most federal government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called ‘APP entities’).

2.37 The APPs provide guidance as to how APP entities handle, use and manage personal information. While the APPs are not prescriptive, each APP entity must consider how the principles apply to its own situation. The principles cover:

- the open and transparent management of personal information including having a privacy policy,
- an individual having the option of transacting anonymously or using a pseudonym where practicable,

---


- the collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection,
- how personal information can be used and disclosed (including overseas),
- maintaining the quality of personal information,
- keeping personal information secure, and
- rights for individuals to access and correct their personal information.36

2.38 The APPs do not apply to local councils or to state or territory governments,37 however most states and territories have privacy laws that apply to state government entities and local councils (South Australia and Western Australia are the only jurisdictions without privacy legislation).

2.39 For example, the Information Privacy Act 2014 (ACT) regulates how personal information is handled by Australian Capital Territory (ACT) public sector agencies. This Act includes a set of Territory Privacy Principles (TPPs), which cover the collection, use, storage and disclosure of personal information, and an individual’s access to and correction of that information.38

2.40 The Department of Home Affairs explained that it is proposed that states and territories without privacy legislation, South Australia and Western Australia, comply with the APPs in relation to their use of the identity-matching services.39

**Stakeholder concerns**

2.41 Submitters raised a number of concerns in relation to the interaction of the IMS Bill with the APP’s. In particular, the APPs provide that individuals should be aware of the reason for collection of their personal information, and that information should only be used for that particular purpose. The

---


ALHR and the AHRC both expressed concern that the IMS Bill does not appear to comply with this as it allows for personal information to be used or disclosed for purposes regardless of the purpose for which it was collected.  

2.42 Further concerns were raised about the extent of access that private sector organisations will have to identity-matching services. In particular the ALHR raised oversight and compliance concerns, noting that APP entities are not subject to regular oversight.

2.43 In its submission, the Office of the Australian Information Commissioner (OAIC) noted that the bills will ‘enable the sharing of identification information of the vast majority of individuals living in Australia’ and also that ‘the identity-matching services will enable the transmission of identification information at a much faster rate than is currently possible’. Given the effect of these changes, the OAIC stated that the ‘bills should be drafted as narrowly as possible to achieve their objectives while minimising the adverse impacts on privacy rights and obligations’.

2.44 The OAIC also provided technical advice on the intersection of ‘identification information’ (as defined in the IMS Bill) and the Privacy Act. The Privacy Act applies different levels of protection to ‘sensitive information’ and ‘personal information’, with the former receiving a higher level of protection. The OAIC advised the Committee that ‘identification information’ as conceived in the IMS Bill would span both types of information as defined in the Privacy Act. More specifically, the OAIC advised that biometric information shared through the interoperability hub would be classified as ‘sensitive information’ under the Privacy Act and thereby engage a more stringent level of protection under that Act.

2.45 Further, the OAIC explained that entities regulated by the Privacy Act are generally not permitted to collect, use or disclose personal information for a purpose other than the purpose for which the information was collected—unless an individual has consented or an exception applies.

---

42 Office of the Australian Information Commissioner, Submission 13, p. 3.
43 Office of the Australian Information Commissioner, Submission 13, p. 2.
2.46 The IMS Bill and Passports Amendment Bill propose to invoke an exception to the collection, use and disclosure of personal information (although the principles relating to information security, information quality and information governance would still apply).\(^{44}\)

**Privacy protections envisaged in the Intergovernmental Agreement**

2.47 The IGA sets out that there are intended to be ‘robust privacy safeguards’ for the design and operation of the identity-matching services. The IGA states that privacy safeguards will be ‘informed by independently conducted privacy impact assessments [and] developed in consultation with federal and state privacy commissioners (or equivalents)’. These safeguards are intended to ‘balance privacy impacts against the broader benefits to the community from sharing and matching identity information’.\(^{45}\)

2.48 As mentioned earlier, the National Security Coordination Group (with representatives from the Commonwealth, states and territories) will oversee the development, implementation and ongoing operation of multifaceted privacy and security safeguards. This includes the Face Matching Services Participation Agreement and Access Policies previously discussed in Chapter 1.\(^{46}\)

2.49 The Participation Agreements and Access Policies ‘will outline the privacy safeguards with which requesting agencies are required to comply while supporting information sharing across jurisdictions’.\(^{47}\) These include:

- providing a statement of the legislative authority or basis on which the Agency may obtain identity information through the Face Matching Services,
- being subject to a privacy impact assessment which includes consideration of the Agency’s use of the Face Matching Services, except where the Agency’s use of the Face Matching Services is expressly exempt from relevant Commonwealth, State and Territory privacy legislation,

---


• entering into arrangements for the sharing of identity information with each Data Holding Agency it wishes to receive information from, within the framework of the Participation Agreement,
• providing appropriate training to personnel involved in the use of the Face Matching Services, and
• conducting annual compliance audits, in a manner to be determined by the Coordination Group, in relation to use of the Face Matching Services.  

2.50 The IGA also provides that agencies and organisations will be subject to oversight by the relevant privacy regulatory or oversight body within their jurisdiction. This includes the OAIC for organisations and government agencies subject to the Privacy Act.  

2.51 In addition, the IGA states that access to state or territory data for private sector users will also be subject to further safeguards, including:
• the express approval of the relevant minister(s) in each state or territory to use their jurisdiction’s information for this purpose,
• the outcomes of a privacy impact assessment covering the types of organisations to be given access to the service,
• compliance with a Facial Verification Service (FVS) Commercial Service Access Policy developed by the National Security Coordination Group, including a fee for service arrangement, and
• an FVS Commercial Service audit and compliance programme overseen by the National Security Coordination Group.  

2.52 The Law Council of Australia, observed that the IGA envisaged robust privacy safeguards, noting

this reflects recognition by governments that Australian citizens expect that derogations from their right of privacy should be justified by governments as aimed at a legitimate objective and be reasonable and proportionate.  

2.53 Submitters indicated concerns that the privacy protections in the IGA are not available for review. The Law Council noted that since access policies and

---

48 COAG, Intergovernmental Agreement on Identity Matching Services, 5 October 2017, p. 22.
49 COAG, Intergovernmental Agreement on Identity Matching Services, 5 October 2017, p. 23.
50 COAG, Intergovernmental Agreement on Identity Matching Services, 5 October 2017, p. 22 and Department of Home Affairs, Submission 12, p. 12.
51 Mr Morry Bailes, President, Law Council of Australia, Committee Hansard, Melbourne, 3 May 2018, p. 15.
data sharing arrangements supporting the implementation of the IMS Bill have not been provided by the government for review, ‘it is unclear what the terms of those policies and agreements will contain’.\(^{52}\)

2.54 Similarly, the OAIC stated that ‘these governance documents are undergoing consultation, and could be subject to change’.\(^{53}\)

**Privacy protections envisaged in the Identity-matching Services Bill 2019**

2.55 The IMS Bill only provides privacy safeguards to local government and non-government entities’ use of identity-matching services.\(^ {54}\)

2.56 These specific provisions are discussed in more detail in Chapter 4 of this report however, generally, local government authorities and non-government entities can request an identity-matching service where:

- the Privacy Act applies to the local government authority or non-government entity, or
- where the local government authority is bound by a law of the State or Territory, or
- the local government authority or non-government entities has entered into a written agreement with the Department of Home Affairs that is comparable to the protection under the APPs.

2.57 Noting that the privacy protections are expected to be established in the Participation Agreement, the OAIC argues that the IMS Bill should be the primary source of privacy protection measures, supported by relevant governance documents and arrangements.\(^ {55}\)

**Other human rights concerns**

2.58 In addition to privacy, other human rights are engaged by the Bills.

2.59 The IMS Bill’s *Statement of Compatibility with Human Rights* indicates that the Bill engages the right to freedom of expression contained in Article 19 of the

---

\(^{52}\) Law Council of Australia, *Submission 8*, p. 6.

\(^{53}\) Office of the Australian Information Commissioner, *Submission 13*, p. 3.

\(^{54}\) IMS Bill, proposed sections 7(2)-(4) and 10(2); see also Department of Home Affairs, *Submission 12*, p. 12.

ICCPR. Both Bills’ Statements recognise that the Bills engage right to liberty and security of the person contained in Article 9 of the ICCPR.\textsuperscript{56}

2.60 Freedom of expression is engaged by the offence in section 22 of the IMS Bill where an employee or a contractor working on behalf of the Department of Home Affairs is prevented from disclosing protected information. The Statement concludes that such a limitation is ‘proportionate to protect the privacy of individuals’, is a key privacy safeguard of the IMS Bill and is ‘proportionate to the need to protect national security and public order by limiting the disclosure of information related to investigations or operations’.\textsuperscript{57}

2.61 In relation to the right to liberty and security of the person, the IMS Bill’s Statement concludes that by ‘helping agencies to fight identity crime and make it more difficult for people to obtain and use fraudulent identities, the Bill will have positive impacts on the liberty and physical security of Australians’.\textsuperscript{58}

2.62 Similarly, the Passports Amendment Bill’s Statement concludes that ‘by making fraudulent identities more difficult to obtain and to use, and by improving the ability of law enforcement agencies to detect fraudulent identities in a timely manner, the Bill will help reduce such negative impacts on personal liberty’.\textsuperscript{59}

2.63 The AHRC stated that the IMS Bill is ‘likely to interfere with a number of other rights’.\textsuperscript{60} These are freedom of movement,\textsuperscript{61} the right to non-discrimination,\textsuperscript{62} and the right to a fair trial.\textsuperscript{63}

\textsuperscript{56} IMS Bill, Explanatory Memorandum, pp. 43, 57; Passports Amendment Bill, Explanatory Memorandum, pp. 6-7.

\textsuperscript{57} IMS Bill, Explanatory Memorandum, p. 57.

\textsuperscript{58} IMS Bill, Explanatory Memorandum, p. 58.

\textsuperscript{59} Passports Amendment Bill, Explanatory Memorandum, p. 7.

\textsuperscript{60} Australian Human Rights Commission, Submission 11, p. 10.

\textsuperscript{61} Article 12 of the ICCPR.

\textsuperscript{62} Article 3 of the ICCPR provides an accessory non-discrimination principle. It is an accessory in that it cannot be used independently and can only be relied upon in relation to another right protected by the ICCPR.

\textsuperscript{63} Article 14 of the ICCPR.
In addition, ALHR submitted that the IMS Bill ‘will necessarily have a chilling effect upon the right of peaceful assembly’,\(^\text{64}\) and that the Passports Amendment Bill ‘may have an adverse impact upon the right of equal access to public service’\(^\text{65}\) and to equality before the law and equal protection of the law’.\(^\text{66}\)

The Human Rights Law Centre address the IMS Bill’s intersection with freedom of movement, stating that facial recognition technology, particularly real-time facial recognition, risked transforming ‘public space into a sphere where each person can be monitored and identified’.\(^\text{67}\)

In relation to freedom of movement the AHRC referred to the fact that, in order to travel abroad, an Australian citizen will need to get a passport and may be required to provide personal identifiers or other information which may be collected by the Department of Home Affairs and made available for use by the identity-matching services.\(^\text{68}\)

The AHRC’s concerns around the right to non-discrimination stemmed from the ability of the Minister to make rules to allow other biometrics to be used in the provision of identity-matching services. According to the AHRC these other biometrics may not be usable by a range of people. It is therefore essential that in all cases where biometric systems are employed to verify identity in the course of accessing a service, alternatives are provided to ensure that people are able to access that service on an equal basis.\(^\text{69}\)

Regarding the right to a fair trial, the AHRC noted that the intended prohibition on using an identity-matching service as the sole basis for ascertaining an individual’s identity for evidentiary purposes in judicial proceedings (which is referred to in the IGA), is not included in the IMS Bill.\(^\text{70}\) Therefore the Bill does not restrict agencies from ‘attempting to use the results of these services in that way’.\(^\text{71}\)

\(^\text{64}\) Article 21 of the ICCPR.
\(^\text{65}\) Article 25 of the ICCPR.
\(^\text{66}\) Article 26 of the ICCPR. Australian Lawyers for Human Rights, *Submission 2*, p. 3.
\(^\text{67}\) Human Rights Law Centre, *Submission 16*, p. 10.
If the prosecution in a criminal proceeding sought to use identity-matching service results to ascertain an individual’s identity, a defendant would be in a difficult position to properly challenge the results obtained from those services.\textsuperscript{72} The AHRC stated that consideration should be given to ‘what, if any, use results derived from identity-matching services should be able to be put in judicial proceedings’.\textsuperscript{73}
3. Identity-matching services, the interoperability hub and the National Drivers License Recognition Solution

3.1 In addition to the general privacy concerns regarding the use, reliability and security of biometric information discussed in the preceding chapter, stakeholders expressed concern regarding technical components of the IMS Bill. These concerns chiefly related to what is collected, how information is used and who has access.

3.2 This chapter discusses proposed sections 5 to 15 of the IMS Bill, which define identity information, the identity-matching services, and provide for the development and operation of the interoperability hub and the National Driver Licence Facial Recognition Solution (Driver Recognition Solution).\(^1\)

3.3 First, the chapter examines the scope and purpose of identity-matching information, including the definition of key terms used throughout the IMS Bill. Second, the access points for the identity-matching services (the ‘interoperability hub’ and the Driver Recognition Solution) will be

---

1 The National Driver Licence Facial Recognition Solution is referred to in the IMS Bill as NDLFRS.
discussed, with the evidence received on each identity-matching service presented. The chapter also presents evidence on the proposed access to the services for local governments and non-government entities.

3.4 The Committee’s comment and recommendations for amendment appear at the end of the chapter.

Scope and purpose of identity-matching services

3.5 As discussed in Chapter 1, under the IMS Bill, the Department of Home Affairs will be able to collect ‘identification information’ for the purposes of providing identity-matching services. While the term is expressly defined in IMS Bill, it is proposed that the Minister will also have a rule-making power to expand the definition of ‘identification information’ where it will assist in an ‘identity or community protection activity’. Further, the Department will be able to collect and disclose that ‘identification information’ through the interoperability hub or the Driver Recognition Solution to users of the service, (including government and, in some cases, non-government entities). The Department may only share identification information for an express range of purposes, including an ‘identity or community protection activity’.

3.6 Therefore, the following terms are central to the Bill’s scope and purpose:

- ‘identification information’—that is, what information may be collected, and
- ‘identity or community protection activity’—that is, for what purpose can information be collected and shared through the interoperability hub and Driver Recognition Solution.

3.7 The following sections of this chapter discuss these key terms in detail as well as who will have access to, and how they will access, biometric information.

Identification information

3.8 Proposed subsection 5(1) of the IMS Bill defines ‘identification information’ as any of a number of attributes about an individual (whether living, dead, real or fictitious). This includes an individual’s name, current or former address, date of birth and gender. An individual’s facial image, and information contained in driver’s licences, other licences, documents

---

2 Identity-matching Services Bill 2019 (IMS Bill), Explanatory Memorandum, p. 11.
provided to people who are not Australian citizens, and travel documents such as passports, are also included in the definition.

3.9 The IMS Bill allows for additional items of ‘identification information’ to be prescribed under the rule-making power contained in proposed section 5(1)(n).

3.10 Proposed subsection 5(2) provides that a number of attributes—including racial or ethnic origin, political opinions, religious beliefs or affiliations or sexual orientation or practices—are not identification information about an individual. However, this would not prevent ‘identification information’ from being used to identify a person where that information could also infer an attribute listed in proposed subsection 5(2). For example, even if an individual’s racial or ethnic origin can reasonably be inferred from his or her name or place of birth, this does not prevent his or her name or place of birth from being ‘identification information’.

3.11 Proposed subsection 5(4) provides that, before making rules prescribing additional ‘identification information’, the Minister must consult the Human Rights Commissioner and the Information Commissioner. The Minister must also be satisfied that the information,

- can be used to identify an individual,
- is reasonably necessary to provide one or more identity-matching services, and
- assists one or more ‘identity or community protection activities’.

3.12 The term ‘identity or community protection activities’ is discussed in the next section.

3.13 Submitters raised concerns with this broad rule making power. The Law Council of Australia was concerned that the rule making power could be used to enhance the scope of the identity-matching services. Additionally, the Law Council submitted that it is not enough that the Human Rights Commissioner and the Information Commissioner are only consulted. The Law Council considered that the Minister should be required to report to the public on the results of these consultations and provide reasons if rules are made that are contrary to the advice provided by the Commissioners.

---

3 Law Council of Australia, Submission 8, p. 5.

4 Law Council of Australia, Submission 8, p. 5.
3.14 In a submission to this Committee’s review, the Department of Home Affairs advised that, as a result of comments made by the Senate Standing Committee for the Scrutiny of Bills, the Minister has agreed to ‘seek to amend’ the IMS Bill to,

- require the Minister to have regard to submissions made by the Human Rights Commissioner and the Information Commissioner when making rules to prescribe additional types of identification information or new identity-matching services, and
- require the Minister to provide reasons explaining why the rules depart from that advice (if they do).

3.15 The Australian Human Rights Commission (AHRC) recommended that the rule making power in subsection 5(1)(n) not be included in the Bill. In making this recommendation, the AHRC noted its particular concerns in relation to the definition of ‘identity or community protection activities’, as discussed below.

3.16 Electronic Frontiers Australia (EFA) also recommended that subsection 5(1)(n) be removed because ‘new types of identification information and new types of identity-matching services ought not merely be subject to prescription by the Minister’. EFA went on to explain that it should be up to the legislature to decide, with proper debate, the basis for further inclusion of new and emerging technologies.

3.17 In discussing the Minister’s power in subsection 5(1)(n), the Department of Home Affairs noted that this Committee expressed significant concerns about a regulation-making provision in its Advisory Report on the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014.

3.18 However, the Department distinguished the current IMS Bill from the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill, pointing out that,

- the IMS Bill will not facilitate the collection from individuals of any new type of biometric data that may be prescribed in the rules—that is, it

---

6 Department of Home Affairs, Submission 12, p. 8.
7 Australian Human Rights Commission, Submission 11, p. 4.
8 Electronic Frontiers Australia, Submission 40, p. (6).
‘will not provide for the collection of biometric information directly from individuals’,

- proposed subsection 5(4) contains a number of additional safeguards that ‘will help to ensure rules are only made in appropriate circumstances and are subject to proper oversight’, and
- proposed subsections 30(3) and (4) of the IMS Bill specifically provide for the rules to be subject to disallowance by Parliament and sunsetting arrangements.\(^9\)

### Identity or community protection activity

3.19 As noted above, before making rules prescribing additional ‘identification information’ under paragraph 5(1)(n), the Minister must be satisfied that the information assists one or more ‘identity or community protection activities’. Further, the Department of Home Affairs will only be able to collect ‘identification information’ through the operation of the interoperability hub or the Driver Recognition Solution for an ‘identity or community protection activity’.

3.20 Proposed section 6 defines ‘identity or community protection activity’ as comprising the following activities:

- preventing and detecting identity fraud,
- law enforcement activities,
- national security activities (including ‘gathering intelligence’) within the meaning of the *National Security Information (Criminal and Civil Proceedings) Act 2004*,
- protective security activities,
- community safety activities,
- road safety activities, and
- verifying identity.

3.21 The Department’s collection of certain biometric information is further restricted to a more limited range of identity or community protection activities. The Explanatory Memorandum notes that the Face Identification Service will not be available for either road safety activities or verifying identity activities.\(^{10}\) Road safety activities are intended to refer to the ability to detect unlicenced and disqualified drivers, persons with multiple licences

---


\(^{10}\) IMS Bill, Explanatory Memorandum, pp. 9,19.
obtained fraudulently and the strengthening of the integrity of driver licence issuance processes.\textsuperscript{11}

3.22 The Explanatory Memorandum states that the verifying identity activities covered in proposed section 6 are intended to capture government or private sector service delivery where it is necessary to establish identity, such as ‘seeking government benefits, requesting a bank account, or where regulatory identity verification requirements exist’.\textsuperscript{12}

3.23 The AHRC raised three main concerns with the breadth of the definition of ‘identity or community protection activity’. The AHRC’s first concern was with the definition of ‘law enforcement activities’ in proposed subsection 6(3)(a), which includes ‘preventing, detecting, investigating or prosecuting an offence against a law of the Commonwealth, a State or a Territory’. The AHRC submitted that allowing the identity-matching services to be used in this way

\textit{appears to contemplate intrusive surveillance of persons (or, indeed, of the community at large) before any crime has been committed, and indeed potentially before there is any reason to believe that a particular crime will be committed.}\textsuperscript{13}

3.24 The Department of Home Affairs, responding to similar concerns expressed in a submission to a separate Queensland inquiry, stated that the IMS Bill ‘does not authorise other agencies to undertake mass surveillance’. The Department noted:

\begin{quote}
The Australian Privacy Principles will continue to operate to prohibit collection, use or disclosure of personal information that is not authorised by law •

Participating agencies need to have their own legal basis to collect information that they wish to use in a query or receive in response to a query, and to share it in the course of one or more of the identity and community protection activities, before they can use the services.\textsuperscript{14}
\end{quote}

3.25 The Department also considered that use of the face-matching services for such blanket surveillance

\textsuperscript{11} IMS Bill, Explanatory Memorandum, p. 19.
\textsuperscript{12} IMS Bill, Explanatory Memorandum, p. 19.
\textsuperscript{14} Department of Home Affairs, \textit{Submission 12}, p. 13.
would not be feasible in practice, given that the systems supporting the services are not designed to support this type of usage and that agencies would not have the resources, including personnel sufficiently trained in facial recognition, to devote to this kind of usage.\(^\text{15}\)

3.26 Secondly, the AHRC expressed concern that the range of information that could conceivably assist in ‘gathering intelligence’ is very broad.\(^\text{16}\) Thirdly, the AHRC stated that ‘verifying the identity of individuals’ could not justify the use of the identity-matching services alone. The Commission considered that the measures could only be justified ‘by reference to some other aim—that is, if the verification is performed to serve some other legitimate purpose’.\(^\text{17}\)

3.27 The AHRC recommended that the definition of ‘identity or community protection activity’ be amended so that ‘law enforcement activities’ includes only the prevention of serious offences, and that subsections dealing with ‘road safety activities’ and ‘verifying identity’ be deleted.\(^\text{18}\)

3.28 Mr Fergus from the Australian Strategic Policy Institute (ASPI), submitting in his private capacity, similarly stated that these definitions should be more narrowly defined.\(^\text{19}\)

3.29 Since the IMS Bill was introduced to the Parliament the passage of the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 (EFI Act) inserted a new definition of national security in section 90.4 of the Criminal Code. This definition is more constrained than that in proposed section 6(4) of the IMS Bill which defines the term ‘national security’ by reference to the National Security Information (Criminal and Civil Proceedings) Act 2004 (NSI Act).

3.30 In the NSI Act, ‘national security’ is defined as ‘Australia’s defence, security, international relations or law enforcement interests’.\(^\text{20}\) In the EFI Act, ‘national security’ is defined as:

- the defence of the country;

---

\(^{15}\) Department of Home Affairs, Submission 12, p. 13.

\(^{16}\) Australian Human Rights Commission, Submission 11, p. 19.

\(^{17}\) Australian Human Rights Commission, Submission 11, p. 19.

\(^{18}\) Australian Human Rights Commission, Submission 11, p. 37.

\(^{19}\) Mr Fergus Hanson, Australian Strategic Policy Institute, Submission 18, p. 2.

- 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 90.4(2);
- the protection of the integrity of the country’s territory and borders from serious threats;
- the carrying out of the country’s responsibilities to any other country or an activity covered by subsection (2);
- the country’s political, military or economic relations with another country or other countries.\(^{21}\)

3.31 Subsection 90.4(2) includes espionage, sabotage, terrorism, political violence, foreign interference, or 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.

3.32 The Committee asked the Department of Home Affairs if the IMS Bill could be amended so that the definition of ‘national security’ in section 6(4) refers to section 90.4 of the *Criminal Code*. The Department stated that definitions were ‘in substance almost the same’\(^{22}\) and offered no objection to the *Criminal Code* definition being used.

**Use of identity-matching services**

3.33 Proposed section 7(1) of the IMS Bill defines ‘identity-matching service’, which includes each of the separately defined services in proposed sections 8–12 (discussed below). In addition, proposed section 7(1)(f) gives the Minister the power to prescribe a new identity-matching service where that service involves the collection, use and disclosure of identification information; and involves the interoperability hub or the Driver Recognition Solution.

3.34 The Minister may only make rules for the purposes of paragraph (7)(1)(f) prescribing a service that ‘involves a request, from a local government authority or non-government entity, relating to an individual’ if

(a) the purpose of the service is to verify the individual’s identity; and
(b) the conditions in subsection (3) are met in relation to the local government authority or non-government entity. These conditions are described below.

\(^{21}\) *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*, section 90.4

\(^{22}\) Department of Home Affairs, *Supplementary Submission 12.3*, p. 10.
Submitters raised concerns around the Ministerial power to prescribe additional identity-matching services. For example, the Office of the Information Commissioner (Queensland) echoed concerns in relation to blanket surveillance and, whilst accepting that it would not be the Government’s intention for the identity-matching services to be used in such a way, stated that ‘the broad power in section 7(1)(f) could potentially facilitate such a use.’

Likewise, the AHRC submitted that the rule making power in proposed section 7(1)(f) must be read in conjunction with the rule making power contained in section 5(1)(n), discussed above. Taken together, these powers ‘could give the Minister the power to create new identity-matching services which are far more intrusive on privacy than those explicitly created by the Bill.’

The AHRC’s position was that any new identity-matching service should only be created by amending relevant legislation. The AHRC therefore recommended that the rule making power in proposed section 7(1)(f) not be included in the IMS Bill.

Accessing identity-matching services

The IMS Bill establishes two access points for the identity-matching services: an ‘interoperability hub’ and the Driver Recognition Solution. Both are discussed below.

Interoperability hub

Proposed section 14 of the IMS Bill provides for the Secretary of the Department to develop, operate and maintain a facility (the interoperability hub) for relaying electronic communications between bodies and persons for the purposes of requesting and providing identity-matching services.

The Explanatory Memorandum gives further information on the expected operation of the interoperability hub stating that it operates via a ‘hub and spoke’ architecture. Participating entities at the ‘spokes’ either provide or

---

Office of the Information Commissioner (Queensland), Submission 3, p. 3.

Australian Human Rights Commission, Submission 11, p. 28.

Australian Human Rights Commission, Submission 11, p. 28.

Australian Human Rights Commission, Submission 11, p. 4.
request information on a query and response basis. The interoperability hub acts as a router to relay identification information between them. Unlike the Driver Recognition Solution, the hub does not permanently store identification information.27

3.41 Dr Marcus Smith noted that facial images will remain with the states and territories or, in the case of passport photos, with the Department of Foreign Affairs and Trade. Dr Smith stated that the interoperability hub could ‘be searched as though the images were held in a Commonwealth database’ and that ‘this approach may, for practical purposes, have the same effect as if the data were held by the Commonwealth’.28

3.42 The Law Council of Australia was concerned that the ‘identity matching services operating through the interoperability hub will use information taken for a particular purpose for other purposes for which the consent of individuals has not been obtained.’ The Law Council gave the example of someone who has consented to providing a photograph for a driver licence ‘but have not consented to their biometric information being extracted from that image and being used for other purposes’. This, according to the Law Council, ‘may have the effect of undermining the notion of informed consent by individuals in relation to their personal information’.29

3.43 The Law Council of Australia was concerned about the sensitivity of personal information flowing through the interoperability hub and the consequences of potential breaches of the hub. The Council pointed out that any ‘inadvertent release, or breach in the security of biometric information is irrevocable’.30

National Driver Licence Facial Recognition Solution

3.44 Proposed section 15 of the IMS Bill provides for the Secretary of the Department to develop, operate and maintain the Driver Recognition Solution. This consists of a database of identification information that is also contained in government identification documents issued by or on behalf of an authority of a state or territory, is supplied by the authority or its agent to the Department by electronic communication for inclusion in the database.

27 IMS Bill, Explanatory Memorandum, p. 28
28 Dr Marcus Smith, Submission 17, p. 3.
29 Law Council of Australia, Submission 8, p. 3.
30 Law Council of Australia, Submission 8, p. 4.
In addition, the Secretary can develop, operate and maintain a system for biometric comparison of facial images with facial images that are in the database.

3.45 According to the Explanatory Memorandum, the database is first expected to hold driver licences but identification information from other state or territory identification documents, such as fishing, firearm and marine licences and proof of age or identity cards, may also be incorporated into the database.\(^{31}\)

3.46 The Explanatory Memorandum provides further detail on how facial matching will work in the Driver Recognition Solution. Following receipt of a matching request, the facial recognition system will create a biometric template from the facial image that is submitted. This biometric template is compared against the templates stored in the system. Once a matching request has been processed, the probe image and its associated templates are not retained anywhere in the Driver Recognition Solution.\(^{32}\)

**The range of identity-matching services**

3.47 As noted in Chapter 1, each identity-matching service is defined in the IMS Bill. The listed identity-matching services include:

- Face Identification Service,\(^{33}\)
- Facial Recognition Analysis Utility Service,\(^{34}\)
- Face Verification Service,\(^{35}\)
- Identity Data Sharing Service,\(^{36}\) and
- One Person One Licence Service.\(^{37}\)

---

\(^{31}\) IMS Bill, Explanatory Memorandum, p. 29.

\(^{32}\) IMS Bill, Explanatory Memorandum, p. 29.

\(^{33}\) Referred to in the IMS Bill as the FIS (proposed sections 7-8).

\(^{34}\) Referred to in the IMS Bill as the FRAUS, referred to in this report as the Facial Recognition Service (proposed sections 7, 9).

\(^{35}\) Referred to in the IMS Bill as the FVS (proposed section 7, 10).

\(^{36}\) Referred to in the IMS Bill as the IDSS; referred to in this report as the Identity Sharing Service (proposed sections 7, 11).

\(^{37}\) Referred to in the IMS Bill as the OPOLS; referred to in this report as the One Licence Service IMS Bill (proposed sections 7, 12).
Submitters raised broad concerns around these services as a whole. The AHRC noted that features of the Face Identification Service are not described in the Bill, that the Bill does not make clear how the Facial Recognition Service operates, that no detail on the Face Verification Services is included in the Bill, and that important features of the One Licence Service are ‘not mandated’ by the Bill.\footnote{Australian Human Rights Commission, Submission 11, pp.22-23, 27.}

In light of this, the AHRC recommended that ‘the provisions defining each of the identity-matching services should be substantially redrafted, so that their functionality is fully defined in the Bill’.\footnote{Australian Human Rights Commission, Submission 11, p. 3.}

Similarly the Law Council was of the view that ‘additional technical information about the nature of the identity matching services and the process for ensuring that there are not false matches should be released publicly to allow informed debate about the proposed legislation’.\footnote{Law Council of Australia, Submission 8, p. 4.}

Likewise, Future Wise and the Australian Privacy Foundation stated that the identity-matching services ‘comprise the tools of big data in the hands of government, with limited oversight only’.\footnote{Future Wise and Australian Privacy Foundation, Submission 1, p. 4.}

Mr Fergus Hanson stated that ‘for all identity checking, the minimum amount of personal information necessary should be exchanged.’\footnote{Mr Fergus Hanson, Australian Strategic Policy Institute, Committee Hansard, Canberra, 17 August 2018, p. 13.}

Stakeholders also made comment on specific identity-matching services. Each of these is examined in further detail in the following sections.

**Face Identification Service**

Proposed subsection 8(1) of the IMS Bill provides that a Face Identification Service involves electronically comparing a facial image of an individual, and other identification information (if any) about the individual, and identification information about one or more individuals that is contained in one or more government identification documents of one or more kinds specified in the request.
3.55 The comparison must be for the purpose of identifying the individual, or determining whether the individual has multiple identities, in the course of an identity or community protection activity.

3.56 The identity or community protection activity for which the Face Identification Service can be used is restricted to preventing or detecting identity fraud, law enforcement, national security, protective security and community safety.\(^{43}\)

3.57 The Explanatory Memorandum explains that the Face Identification Service is a ‘one-to-many’ facial matching service where a facial image and, where known, other biographic information, is submitted for matching against a specific database through the interoperability hub. The facial matching process, consisting of two stages, will first return a small gallery of the highest matching facial images in the database. After the receiving agency has reviewed the gallery and selected a shortlist of possible matches, they will then have access to the biographic details associated with the facial images on their shortlist, for further examination.\(^{44}\)

3.58 According to the Explanatory Memorandum, providing images via the interoperability hub will mean that this service is restricted to one or more of the databases connected to the interoperability hub. That is, it will not be able to be used to compare a facial image against other facial images not contained in government identification documents, for example a database of CCTV images. Details of requests for the Face Identification Service will be subject to audit logging within the interoperability hub, to improve accountability.\(^{45}\)

3.59 Subsections 8(2)(a) to (p) provides that law enforcement, anti-corruption and Australian Government Departments administering the Australian Citizenship Act 2007, the Australian Passports Act 2005, the Foreign Passports (Law Enforcement and Security) Act 2005 and the Migration Act 1958 may request the provision of the Face Identification Service. Importantly, the service would not be available to non-government entities, and only available to those specifically listed in the primary legislation.

\(^{43}\) IMS Bill, Explanatory Memorandum, p. 22. These ‘identity or community protection’ activities are defined in section 6(2)-(6).

\(^{44}\) IMS Bill, Explanatory Memorandum, p. 22.

\(^{45}\) IMS Bill, Explanatory Memorandum, p. 22.
3.60 Proposed subsection 8(2)(q) provides that ‘an authority prescribed by the rules’ may also request the provision of the Face Identification Service. The Explanatory Memorandum explains that, in relation to ‘an authority prescribed by rules’ the power is ‘solely intended to allow these agencies to continue using the [Face Identification Service] following a machinery of government, name or legislative change, without having to amend the Act’.47

3.61 Proposed subsection 8(3) provides that before the Minister makes rules prescribing access to the Face Identification Service, 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 in subsections 8(2)(a) to (p).

3.62 Submitters raised specific concerns that there are not sufficient controls on the use of the Face Identification Service and that the provision do not reflect the IGA.

3.63 The AHRC referred to the process outlined in the Explanatory Memorandum (quoted above), and argued that the controls are insufficient, stating that:

There is nothing in the Identity Bill that controls what use may be made of the information returned at either of the two stages above. It would be possible for the receiving agency to capture and retain it for their own records — or even to compile their own databases of information they receive for future use in unrelated matters. It is relevant to note here that the Identity Bill places no limits on the number of [Face Identification Service] requests that may be made.48

3.64 The Law Council submitted that the Face Identification Service as outlined in the Bill is not in line with the IGA. The Law Council noted that the Face Identification Service ‘has been defined in the Bill to reflect the terms of the [IGA]’, however the Bill ‘does not incorporate the limit that the offence must carry a maximum penalty of not less than three years imprisonment.’ Therefore, the Law Council concludes that the Bill ‘appears inconsistent with the provisions and the spirit of the [IGA]’.49

---

46 IMS Bill, proposed section 8(2)(q).
47 IMS Bill, Explanatory Memorandum, p. 23.
49 Law Council of Australia, Submission 8, p. 7.
3.65 The Queensland Office of the Information Commissioner and the Tasmanian Government also noted this requirement appears in the IGA but not the Bill.\(^{50}\)

3.66 In relation to this concern, the Department of Home Affairs stated that whilst the three-year offence threshold is not in the Bill, ‘it will apply in practice to the sharing of data between jurisdictions, through the application of the provisions in the IGA’.\(^{51}\) The Department further explained that, due to variations in criminal offences across jurisdictions, it is important that there is a degree of flexibility provided to those wanting to access the Face Identification Service. Contradicting the statement that the three-year offence provision will apply in practice, the Department stated that ‘possibly data from other jurisdictions’ could be used ‘for law enforcement purposes where they may have lower penalty for an offence that would meet the ‘penalty threshold’ in other jurisdictions’.\(^{52}\)

3.67 The Committee also received evidence that access to the Face Identification Service should only be available on the issue of a warrant. The AHRC argued that, whilst there may circumstances in which the use of a service such as the Face Identification Service is warranted, ‘the use of such a measure must be strictly controlled to ensure that it is employed only when demonstrated to be justified’ and that it ‘would be appropriate to introduce a warrant regime regulating access’ to the Face Identification Service.\(^{53}\)

3.68 The Queensland Council for Civil Liberties raised concerns regarding ‘absent consent of the individuals involved’ and the need for greater safeguards in relation to the expanded use of biometric data. They argued that access to biometric data for ‘purposes other than those for which it was collected and emergency situations, should be limited to cases where the person seeking access has obtained a warrant from a judicial officer’.\(^{54}\)

3.69 The Department of Home Affairs argued against the need for a warrant to access the Face Identification Service. The Department noted that the

---

\(^{50}\) Queensland Office of the Information Commissioner (QOIC), Submission 3, p. 3; Tasmanian Government, Submission 7, p. 1. The requirement, referred to by the Law Council, the QOIC and the Tasmanian Government is in paragraph 4.21(b) of the IGA.

\(^{51}\) Department of Home Affairs, Submission 12, p. 15.

\(^{52}\) Department of Home Affairs, Submission 12, p. 15.

\(^{53}\) Australian Human Rights Commission, Submission 11, p. 22.

\(^{54}\) Queensland Council for Civil Liberties, Submission 10, p. 2.
Attorney-General’s Department’s Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers of 2011 sets out the circumstances when it would be appropriate to require agencies to obtain a warrant. These are:

- where there is entry to premises without consent,
- where it is required to use reasonable force against things or persons in the execution of a warrant,
- where there is seizure of items, and
- where there is a monitoring regime involving the above matters.\(^{55}\)

3.70 The Department of Home Affairs stated that requiring a warrant to access the Face Identification Service ‘would have a significant impact on the ability of law enforcement or other agencies to use the services in the course of their activities’.\(^{56}\) The Department also argued that the time involved in preparing, reviewing and granting a warrant application would delay and possibly undermine law enforcement and national security investigations, impede operational activity and divert resources from investigations.\(^{57}\)

3.71 The AHRC, responding to the claim that a warrant might negatively impact on enforcement, stating that

warrant regimes can be designed, and in fact currently are designed and operated, to allow for warrants to be obtained very quickly in emergency situations and outside business hours overnight. That is quite possible and feasible, and in fact occurs. So that’s a factor that needs to be taken into account in assessing just how much of an imposition a warrant regime would place on the use of the [Face Identification Service].\(^{58}\)

**Facial Recognition Analysis Utility Service**

3.72 Proposed section 9 of the IMS Bill defines a Facial Recognition Analysis Recognition Service (Facial Recognition Service) as electronically comparing the facial image of an individual (that is included in a request for the

---


57 Department of Home Affairs, *Submission 12*, p. 16.

provision of the service made by an authority of a State or Territory) to a database in the Driver Recognition Solution.

3.73 The comparison must be for the purpose of assessing the accuracy or quality of identification information held by the authority.

3.74 The Facial Recognition Service will allow state and territory road agencies, and other state and territory authorities that may contribute to facial images to the Driver Recognition Solution, to conduct biometric matching using their own data. It allows a state or territory to use the facial recognition capability in the Driver Recognition Solution against their own replicated data. Use of this service will be limited to State and Territory authorities.\(^59\)

3.75 According to the Explanatory Memorandum, the Facial Recognition Service is most likely to be used by ‘road transport authorities to improve the accuracy or quality of its information holdings, for example, to check against the authority’s own records or to detect and replace poor quality photographic images.\(^60\)

3.76 The AHRC state that the Facial Recognition Service did not cause them significant human rights concerns as it is a ‘significantly more limited service’ than others created by the IMS Bill.\(^61\) However, they still raised the concern that the Bill does not make clear precisely how the [Facial Recognition Service] would operate. In particular, it is not clear what information would be supplied in a response to a [Facial Recognition Service] request, and whether it might include information about more than one person. Those matters are not addressed in the secondary materials. The Commission submits that those matters should be clarified in the text of the Bill so that a full assessment of any privacy impacts can be made.\(^62\)

**Face Verification Service**

3.77 Proposed subsection 10(1) defines a Face Verification Service as electronically comparing identification information provided by the person or body making the request with identification information that is contained in a government identification document. The request must specify the kind

---

59 IMS Bill, Explanatory Memorandum, p. 23.
60 IMS Bill, Explanatory Memorandum, p. 24.
of identification document used in the request and the request must include a facial image. The request must be for the purpose of verifying the identity of the individual.

3.78 The IMS Bill provides that the government authorities (Commonwealth, state, territory and local governments) as well as non-government entities may use the Face Verification Service where certain conditions are met.63

3.79 The Explanatory Memorandum provides that, under ‘access policies and data sharing agreements’, the private sector will only be provided with a ‘match or no match’ response, without returning images or biographic information about the person.64

3.80 The Face Verification Service commenced operation in November 2016, enabling the Department of Foreign Affairs and Trade and the Australian Federal Police to access citizenship images held by the then Immigration Department. At the time of the launch it was announced that other types of images such as visa, passport and driver licence photos would be added over time, and that access would subsequently be expanded to other government agencies.65

3.81 The Committee received submissions from the Department of Human Services and the Digital Transformation Agency supporting the implementation of the Face Verification Service.

3.82 The Department of Human Services currently utilises the Document Verification Service to confirm the authenticity of documents. The Document Verification Service informs Departmental decisions that rely on the confirmation of a person’s identity, but it does not identify whether the documents have been obtained fraudulently. Facial verification is currently undertaken manually by the Department through a ‘visual comparison of a physically present individual against the image on their photo identity document.’66

3.83 The Department stated that face biometric technology

---

63 IMS Bill, subsection 7(3).
64 IMS Bill, Explanatory Memorandum, p. 25.
65 M Keenan (Minister for Justice), New face verification service to tackle identity crime, media release, 16 November 2016.
66 The Department of Human Services, Submission 38, p. 2.
has the potential to replace this manual process and strengthen the accuracy of identity confirmation against photo identity documents, such as passports and drivers licences, and therefore reduce the risk of incorrect matching.\textsuperscript{67}

3.84 The Department also stated that the Face Verification Service would assist in confirming a person’s identity where no photographic identification was available, such as following a crisis or emergency. \textsuperscript{68}

3.85 The Digital Transformation Agency submitted that the Face Verification Service would provide efficiencies in providing government services electronically, without the need for an individual having to present in person to a shopfront. \textsuperscript{69}

3.86 However, the Law Council of Australia raised a concern that the ‘match or no match’ response limitation, as mentioned above, is not contained within the IMS Bill. Since access policies and data sharing arrangements supporting the implementation of the Bill have not been provided by the Government for review, they submitted that it is unclear what the terms of those policies and agreements will contain.\textsuperscript{70}

3.87 In addition, the Law Council noted that the provisions of the IMS Bill regarding local government or non-government entities accessing the Face Verification Service do not take into account the caveats on such access set out in the IGA. The IGA states private sector access to the Face Verification Service to match information held by states and territories will be subject to:

(a) the express approval of the relevant minister(s) in each state or territory to use their jurisdiction’s information for this purpose, to be communicated in writing to the Commonwealth at any stage following signature of this Agreement,

(b) the outcomes of a privacy impact assessment covering the types of Organisations to be given access to the service,

(c) compliance with a [Face Verification Service] Commercial Service Access Policy developed by the Coordination Group, including a fee for service arrangement, and

\textsuperscript{67} The Department of Human Services, Submission 38, p. 2.

\textsuperscript{68} The Department of Human Services, Submission 38, p. 3.

\textsuperscript{69} The Digital Transformation Agency, Submission 37, p. 2.

\textsuperscript{70} Law Council of Australia, Submission 8, p. 6.
(d) n [Face Verification Service] Commercial Service audit and compliance programme overseen by the Coordination Group.\textsuperscript{71}

3.88 Mr Fergus Hanson from the Australian Strategic Policy Institute, speaking in his private capacity, raised concerns around the on selling of data linked to a verified identity. He stated:

\ldots with the [Face Verification Service], there needs to be specific provision that if that tool is being used for digital identity purposes, then companies, and government as well, should not be able to gather data linked to that verified identity\ldots In my view the onselling of data should be expressly banned when it's linked to use of the FVS for digital identity purposes.\textsuperscript{72}

Identity Data Sharing Service

3.89 Proposed section 11 of the IMS Bill provides that an Identity Data Sharing Service is disclosure of an individual’s identification information for the purpose of an identity or community protection activity, and it is by one authority of the Commonwealth or state or territory to another authority of the Commonwealth or State or Territory. The Face Identification Service, Facial Recognition Service, Face Verification Service and One Licence are not an Identity Data Sharing Service.

3.90 The Explanatory Memorandum states that the Identity Data Sharing Service allows for the ‘sharing of identification information from one entity to another in a secure and accountable manner through the interoperability hub’, [and] ‘does not involve any facial biometric or other data matching’ but ‘merely transmits identification information from one participating entity to another’.\textsuperscript{73}

3.91 The AHRC acknowledged the need for government to share personal information but stated that the Identity Data Sharing Service regime should not be passed in its current form. The AHRC noted that Identity Data Sharing Service ‘regime as drafted does not specify the circumstances in

\textsuperscript{71} Law Council of Australia, Submission 8, p. 6 quoting Intergovernmental Agreement on Identity Matching Services, 5 October 2017, p. 15.

\textsuperscript{72} Mr Fergus Hanson, Australian Strategic Policy Institute, Committee Hansard, Canberra, 17 August 2018, p. 13.

\textsuperscript{73} IMS Bill, Explanatory Memorandum, p. 26.
which disclosures may be made, nor the extent or types of information that may be disclosed’. 74

3.92 Further, the AHRC argued that ‘laws authorising such disclosures should be precise in their terms and ensure that disclosures will only be possible where necessary and proportionate’. 75 Therefore it is their position that the Identity Data Sharing Service should permit ‘disclosures of information only when necessary, and only to the extent necessary, to achieve a legitimate objective’. 76

One Person One Licence Service

3.93 Proposed section 12 of the IMS Bill provides that a One Licence Service is electronically comparing a facial image of an individual, and any other identification information about the individual, that is included in a request for the provision of the service made by an authority of a state or territory.

3.94 The service would compare the supplied information with identification information held in one of the state or territory databases held in the Driver Recognition Solution. The request may only be made by an agency that issues government identification documents, and the comparison made by the service may only be made against a database that holds government identification documents of the same kind. The comparison must be made for the purpose of determining whether a person holds multiple identification documents of a particular type in one or more states or territories. The request may be made directly to the Driver Recognition Solution, or via the interoperability hub.

3.95 The One Licence Service will allow a state or territory road authority to check if a person has multiple or fraudulent driver licences anywhere in Australia when that person applies for a new licence or renewal of a licence. 77

3.96 The AHRC noted that it did not hold the same concerns about the One Licence Service as the other identity-matching services (such as the Face Identification Service). This is because, like the Facial Recognition Service, the One Licence Service

77 IMS Bill, Explanatory Memorandum, p. 27.
uses information that has been collected for the purpose of issuing drivers’ licences, and uses that information for the purpose of protecting the integrity of the licensing regime. That means that these services are using personal information for purposes connected to the purposes for which the information was collected.\textsuperscript{78}

**Local government or non-government entity requests**

3.97 As noted earlier, the Minister may only prescribe a new identity-matching service that ‘involves a request, from a local government authority or non-government entity, relating to an individual’ if the conditions in proposed subsection 7(3) are met. These conditions are that:

- a verification of the individual’s identity is reasonably necessary for one or more of the functions or activities of the local government authority or non-government entity,
- an individual has consented to the disclosure of identification information, and
- the local government authority or non-government entity either carries on activities in Australia from premises in Australia or resides in Australia.

3.98 In addition proposed subsection 7(3)(d) provides a condition that either the *Privacy Act 1988* applies to the local government authority or non-government entity, or they are bound by a law of a state or territory, or they have entered into a written agreement that meets the requirements set out in subsection 7(4). Proposed section 7(4) requires that the written law or agreement

- protects personal information in a way comparable to the APPs,
- is capable of monitoring, and
- has 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.

3.99 Submitters expressed concerns about how the provision in proposed subsections 7(3) and 7(4) would operate. The Law Council pointed out that that was no indication as to who would be responsible for the ‘monitoring of compliance with the law or agreement’ and that participating agencies who

\textsuperscript{78} Australian Human Rights Commission, *Submission 11*, p. 27.
are not APP entities under the Privacy Act ‘may not be subject to existing audits or independent oversight by external bodies.’

3.100 In addition, the Law Council of Australia argued that the requirement for ‘a means for an individual to seek recourse’ does not provide for that means to be the same as, or equivalent to, the options available to individuals under the Privacy Act. Individuals dealing with a non-APP entity may have a different range of dispute resolution options available to those interacting with an APP entity. The Law Council were concerned that this approach would result in complexity, possible confusion and inadvertent erosion of existing rights.

3.101 Australian Lawyers for Human Rights (ALHR) agreed with the Law Council’s concerns and argued that the proposed protection in proposed subsection 7(4) ‘provides very little protection in practice, particularly where the agreement relates to biometric data which of itself removes one of the key APP rights – to be anonymous or pseudonymous’.

3.102 Proposed subsection 7(5) provides that before making rules for the purposes of paragraph (1)(f), the Minister must consult the Human Rights Commissioner and the Information Commissioner about the proposed rules. Concerns around consultation with the Human Rights Commissioner and the Information Commissioner were discussed above in relation to the rule making power provided for at proposed subsection 5(1)(n).

3.103 Currently, the Bill provides that the only service that a local government authority or non-government entity may request access to is the Face Verification Service.

Consent

3.104 Submitters raised a number of concerns around consent. These included concerns about how consent is given for the access and provision of identity services, the monitoring of such consent, and the use of secondary consent. Secondary consent refers to where a person has consented to use of their identification information for the provision of an identity document (such as a driver licence or passport), and that is then taken as consent for use for another purpose (such as for identity-matching services).

---

79 Law Council of Australia, Submission 8.1 p. 5.
80 Law Council of Australia, Submission 8.1 p. 5.
3.105 ALHR suggested that, if a person’s consent is a pre-condition to the provision of a service, consent given in such circumstances cannot be considered as free and fully informed.\textsuperscript{82}

3.106 The Law Council outlined a similar concern in relation to service provision. After detailing the four elements of consent in the context of the Privacy Act, they conclude that ‘it is unlikely that individuals will have a genuine choice to withhold consent if they wish to obtain the relevant services’.\textsuperscript{83} Further, given that there is no obligation imposed on entities to provide alternative ways of accessing relevant services, ‘consent’ given in such a situation will not satisfy the requirements for consent.\textsuperscript{84}

3.107 The Victorian Government raised concerns around the practicalities of how such consent may be monitored and ‘who would administer the checks and balances in support of this’.\textsuperscript{85}

3.108 In relation to secondary consent, Civil Liberties Australia argued that a person consenting to a driver’s licence photo or passport may be considered to have consented to the use of that photo for a legitimate purpose in relation to it, such as road safety or border security. However, this consent ‘is not a general permission to the state to do whatever it wants with the data.’\textsuperscript{86}

3.109 Similarly the Human Rights Law Centre (HRLC) argued that people who have consented to having their driver licence photo taken are not also ‘providing free, informed and express consent to the Australian Taxation Office to search and obtain their photo when applying for an [Australian Business Number] at indeterminate point in the future’.\textsuperscript{87} The HRLC called for ‘informed debate and careful scrutiny’ of the IMS Bill to ensure that ‘it is targeted and fully justified’.\textsuperscript{88}

\textsuperscript{82} Australian Lawyers for Human Rights, \textit{Submission 2}, p. 7.

\textsuperscript{83} Under section 6(1) of the Privacy Act 1988 consent means ‘express consent or implied consent.’ The four elements of consent are: 1. the individual is adequately informed before giving consent; 2. the individual gives consent voluntarily; 3. the consent is current and specific; and 4. the individual has the capacity to understand and communicate their consent.

\textsuperscript{84} Law Council of Australia, \textit{Submission 8.1} p. 4.

\textsuperscript{85} Victorian Government, \textit{Submission 14}, p. 3.

\textsuperscript{86} Civil Liberties Australia, \textit{Submission 5}, p. 2.

\textsuperscript{87} Human Rights Law Centre, \textit{Submission 16}, p. 9.

\textsuperscript{88} Human Rights Law Centre, \textit{Submission 16}, p. 9.
3.110 Future Wise and the Australian Privacy Foundation echoed this view stating that the IMS Bill represents ‘unacceptable scope creep’, where information collected for one purpose is being used for secondary purposes beyond the scope or conditions supporting its original collection.89

3.111 The Department of Home Affairs stated that the concept of ‘consent’ in the Bill is based on relevant provisions of the APPs in the Privacy Act and comparable state and territory privacy legislation. In relation to consent, the Department stated that the obtaining of consent for use of the Face Verification Service will operate in the same way as it does in the context of the existing Document Verification Service. The Department noted that the Document Verification Service relies on its private sector users meeting the consent and other privacy requirements referred to in the APP Guidelines.90

3.112 Commenting on the issue of accessing services, the Department stated that private sector users of the Face Verification Service will need to meet their obligations under the Privacy Act and this may mean that a private sector organisation would have to provide ‘alternative options for identity verification using the [Document Verification Service] or other identity verification processes if a customer does not consent to the use of their identification information through the [Face Verification Service]’.91

3.113 In relation to secondary consent, the Department stated:

The use and disclosure of personal information for secondary purposes without the consent of an individual is clearly contemplated in certain circumstances under the APPs and comparable state and territory privacy legislation.92

3.114 The Department explained that it does not interact directly with individuals whose information is used in the services as it is merely the ‘facilitator’ of the identity-matching services and the ‘operator’ of the interoperability hub and the Driver Recognition Solution. Therefore the Department considered that it was impracticable for it to ‘collect consent directly from individuals

89 Future Wise and Australian Privacy Foundation, Submission 1, p. 9.
90 Department of Home Affairs, Submission 12.1, p. 6.
91 Department of Home Affairs, Submission 12.1, p. 6.
92 Department of Home Affairs, Submission 12.1, p. 7.
for the secondary use of their information in the identity-matching services’. {93}

3.115 The Department stated that it would rely on APP 6.2(b), which permits use or disclosure where authorised by a Commonwealth, state or territory law – in this the case, the Bill. This will enable the Department to lawfully fulfil its role in transmitting information between agencies participating in the identity-matching services.{94}

3.116 Responding to how local government authorities or non-government entities might demonstrate compliance with conditions relating to consent, the Department stated that in most cases ‘data-holding agencies already have legislative permissions to share identification information without the consent of the individual for some or all of the activities for which the identity-matching services will be available’. {95}

3.117 The Department also undertook to ‘make publicly available information on the operation of the identity-matching services so that the community is aware of and can understand how their information is used through these services’. {96}

**Notices to individuals**

3.118 The Law Council submitted that in order to ‘ensure that users or consumers fully appreciate the basis on which they are providing their identification information’ the IMS Bill should be amended to more accurately refer to a requirement for the relevant local government authority or non-government entity to provide clear notice to individuals of the collection and use of their identifying information. {97}

3.119 The Law Council stated that local government authorities or non-government entities should provide information to individuals whose identities are to be verified using identity-matching services. This should include information about the use of the data including:

---

{93} Department of Home Affairs, Submission 12.1, p. 7.

{94} Department of Home Affairs, Submission 12.1, p. 7.

{95} Department of Home Affairs, Submission 12.1, p. 8.

{96} Department of Home Affairs, Submission 12.1, p. 8.

{97} Law Council of Australia, Submission 8.1 p. 4.
▪ practices undertaken in relation to the face matching services,
▪ the risks to the individual in the event that their biometric data is compromised,
▪ the absence of any enforceable legal remedy if the information is lost or breached,
▪ the jurisdiction and control over the data hosting and usage mechanisms, and
▪ the full list of identity-matching systems which may be able to use this data once collected.98

3.120 In relation to notifying individuals of the use of their identification information in the identity-matching services, the Department stated that notification to individuals will rely to a significant extent on data-holding agencies, including state and territory road agencies, to inform individuals about the intended use of their information in the identity-matching services. The Department will work closely with these agencies to ensure that these notifications are updated as the services come online for different data sources.99

---

98 Law Council of Australia, Submission 8.1 p. 4.
4. Collection, use, protection and disclosure of identification information and reporting and review requirements

4.1 This chapter discusses proposed sections 17-25 of the IMS Bill which provide for the collection, use, disclosure, protection and recording of identification information.

4.2 The chapter then discusses proposed sections 26-30 of the Bill which provide for the delegation of the Secretary’s powers, annual reporting and review of the Bill.

Collection of identification information

4.3 Proposed section 17(1) of the IMS Bill provides that the Department may collect identification information (whether or not it is sensitive information as defined in the Privacy Act 1988) about an individual from someone other than the individual, if the collection is by means of an electronic communication to the interoperability hub or the Driver Recognition Solution.

4.4 Proposed section 17(2) outlines the purposes for which identification information may be collected under subsection (1). These purposes include
providing an identity-matching service for the purpose of an identity or community protection activity, developing identity-matching services, protecting assumed identities and protecting witness identities.

4.5 Proposed section 18 of the IMS Bill provides that the Department may, for any purpose described in subsection 17(2), use or disclose identification information collected by means of an electronic communication to the interoperability hub or the Driver Recognition Solution.

4.6 Proposed section 19 applies if a law of a state or territory limits disclosure of some or all identification information by an authority of a state or territory or by a body or person acting on behalf of such an authority and exempts from the limitation a disclosure authorised by a law of the Commonwealth.

4.7 Proposed section 19(2) further provides that, for the purposes of the exemption, the authority, body or person may disclose to the Department by electronic communication identification information about an individual for inclusion in the Driver Recognition Solution.

Protection of identification information

4.8 Proposed section 21(1) creates an offence, punishable by imprisonment for two years if a person is or has been, an entrusted person; and the person has obtained protected information in his or her capacity as an entrusted person; and, the person makes a record of the information or discloses the information to another person. The fault element for the offence is recklessness.

4.9 Proposed section 21(2) creates exceptions to the prohibitions in proposed section 21(1) where the conduct is authorised by a law of the Commonwealth or of a state or territory or the conduct is in compliance with a requirement under a law of the Commonwealth or of a state or territory. A defendant bears an evidential burden in relation to the matter in 21(2).

4.10 Proposed section 21(3) restricts required disclosure of protected information or production of documents, except where it is necessary to do so for the purposes of giving effect to the Act or the Law Enforcement Integrity Commissioner Act 2006, or a legislative instrument under either Acts. It provides that an entrusted person is not to be required to disclose protected information, or produce a document containing protected information, to a court or a tribunal, authority or person that has the power to require the answering of questions or the production of documents.
Entrusted person is broadly defined in Section 21(4) and includes the Secretary of the Department or an Australian Public Service (APS) employee in the Department. In addition, entrusted persons are those who are contractors engaged in relation to the interoperability hub or the Driver Recognition Solution and are also officers or employees of an agency or authority of the Commonwealth, a state or territory, the government of a foreign country or of a public international organisation.

Protected information is also broadly defined in section 21(4) as:

- identification information that was obtained by a person, in the person’s capacity as an entrusted person, from an electronic communication to or from either the interoperability hub or the Driver Recognition Solution,
- information obtained by a person, in the person’s capacity as an entrusted person about an electronic communication made to or from either the interoperability hub or the Driver Recognition Solution,
- identification information relating to a particular individual held in, or generated using, the Driver Recognition Solution, and,
- information that enables access to the interoperability hub or the Driver Recognition Solution and was obtained by a person, in the person’s capacity as an entrusted person.

Authorised use and disclosure of identification information

Proposed section 22 provides that an entrusted person may make a record of or disclose protected information if the record is made, or the information is disclosed for the purposes of the Act or in the course of exercising powers, or performing functions or duties, relating wholly or partly to the interoperability hub or the Driver Recognition Solution.

Proposed section 23 provides that an entrusted person may disclose protected information if they reasonably believe that the disclosure is necessary to lessen or prevent a serious and imminent threat to the life or health of an individual and the disclosure is for the purpose of lessening or preventing that threat.

Proposed section 24 of the Bill provides that an entrusted person may disclose protected information to the Integrity Commissioner for the purpose of referring an allegation, or information, that raises a corruption issue (within the meaning of the Law Enforcement Integrity Commissioner Act
or for the purpose of notifying a corruption issue under that Act or for the purpose of an investigation of a corruption issue under that Act.

4.16 In both cases an entrusted person may make a record of protected information for the purpose of disclosing the protected information.

4.17 Proposed section 25 provides that an entrusted person may make a record of, or disclose, protected information that relates to the affairs of a person if the person has consented to the recording or disclosure and the recording or disclosure is in accordance with that consent.

Delegation Powers

4.18 Section 27 of the Bill allows that the Secretary of the Department may, in writing, delegate all or any of his or her functions or powers under this Act to a Senior Executive Service (SES) employee or acting SES employee in the Department. In performing a delegated function or exercising a delegated power, the delegate must comply with any written directions of the Secretary of the Department.

Reporting requirements

4.19 Section 28(1)(a) provides that the Secretary of the Department must give the Minister a report on statistics relating to all requests in the financial year, from authorities of the Commonwealth (except the Australian Security Intelligence Organisation (ASIO)) or of a state or territory, for the Face Identification Service, Face Verification Service and One License Service.

4.20 The report must also include statistics relating to all requests in the financial year from non-government entities for a Face Verification Service, and the report is required to include statistics from each authority of the Commonwealth (except ASIO), and each authority of a State or Territory (including a local government authority), that used an Identity Data Sharing Service to disclose or collect identification information in the financial year.

4.21 The Department of Home Affairs informed the Committee that the Minister has agreed to seek to amend the IMS Bill to provide for annual reporting in relation to the number of instances in which an entrusted person discloses

---

1 SES employee and acting SES employee are defined in section 2B of the Acts Interpretation Act 1901.
protected information to lessen or prevent a threat to life or health as provided for in proposed section 23 of the IMS Bill.

4.22 The Explanatory Memorandum notes that ‘non-government entities are not required to be individually named in the report’ as this is ‘necessary to protect commercial confidentiality.’

4.23 In response to this, the Law Council of Australia stated that it considers ‘that the public have a right to know which non-government entities have access to the Face Verification Service.’ Similarly the Office of the Information Commissioner (Queensland) pointed out that

private sector users of the [Face Verification Service] will be required to secure the consent of the individual whose identity they are seeking to verify [s7(3)(b)]. As this would reveal to the individual that the non-government entity is using the [Face Verification Service], it is unclear why the commercial confidentiality of that non-government entity would be compromised by its identification in the annual report.

4.24 In relation to the exceptions to reporting by ASIO, the Explanatory Memorandum states that this is in order to ‘protect the security of their operations’.

4.25 The Law Council argued that such an exception ‘should be determined on a case by case basis’ and should not be included ‘as a blanket exception, particularly in circumstances where ASIO has shared biometric data with international partners.’

4.26 In relation to ASIO’s exclusion for the reporting requirements, the Department expanded on information provided in the Explanatory Memorandum noting that ‘ASIO is exempt from the operation of the Privacy Act and the Freedom of Information Act 1982’ and that ‘ASIO will continue to be subject to its existing oversight regimes, which will apply in relation to ASIO’s use of the identity-matching services. This includes oversight by the Inspector-General of Intelligence and Security.’

---

2 Explanatory Memorandum, p. 37.
3 Law Council of Australia, Submission 8, p. 7.
4 Office of the Information Commissioner (Queensland), Submission 3, p. 5.
5 Explanatory Memorandum, p. 37.
6 Law Council of Australia, Submission 8, p. 7.
7 Department of Home Affairs, Submission 12.1, p. 10.
4.27 Proposed section 28(2) provides that the annual report must not unreasonably disclose personal information about an individual. Proposed sections 28(3) and (4) provide that the Secretary of the Department must give the Minister the report as soon as practicable after the end of the financial year and in any case within 6 months after the end of the financial year and that the Minister must cause a copy of the report to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives the report.

4.28 The Office of the Information Commissioner (Queensland) submitted that additional requirements in annual reporting processes are necessary to ‘adequately monitor privacy impacts, misuse, mistakes and private sector use associated with the IMS regime’. They noted that the IMS Bill ‘does not require data breaches or security incidents (for example through unauthorised access or unauthorised disclosure), system failures or accuracy rates to be reported upon’.\(^8\)

4.29 Noting that management of data breaches is governed by the new data breach notification provisions in Part IIIC of the Privacy Act 1988 the Department of Home Affairs stated that it is ‘not necessary to duplicate data breach reporting by requiring this information to be included in the annual report under the Bill’.\(^9\)

4.30 In relation to other matters, such as security incidents and unauthorised use or disclosure, the Department stated that such reporting may not be appropriate as it may ‘disclose information about the security architecture of the systems’.\(^10\)

4.31 The Department also explained that it ‘may not have information about all instances of unauthorised use or disclosure if these occur at participating agency level’. However the Department noted that ‘this information will be able to be captured, and properly investigated and assessed, through annual audit requirements on participating agencies using the services’ as well as reviews of the services required under the IGA (every three years), and the Bill (a review to be commenced within five years)’.\(^11\)

---

8 Office of the Information Commissioner (Queensland), Submission 3, pp. 4-5.

9 Department of Home Affairs, Submission 12.1, pp. 9-10.

10 Department of Home Affairs, Submission 12.1, p. 10.

11 Department of Home Affairs, Submission 12.1, p. 10.
4.32 In addition, the Human Rights Law Centre (HRLC) raised concerns on the accuracy of facial recognition technology. The HRLC explained that facial recognition technology contains a ‘bias towards the dominant ethnic group in the area in which it is developed’ and, in Australia, the use of such technology could have a disproportionate effect on ‘Aboriginal and Torres Strait Islanders who are overrepresented in arrest and incarceration rates’. Given this concern the annual report should include ‘annual accuracy testing based on demographics’.

4.33 The Committee were interested in the accuracy of the technology and inquired about the vendor supplying biometric facial recognition algorithms. The Department of Home Affairs explained that it did not report the identity of vendors in order to reduce ‘the potential vectors of attack’ and that as all biometric facial recognition providers use different algorithms, naming them would potentially create ‘an increased threat of attack’.

4.34 In response to a question about possible publication of performance figures in order to provide a level of public assurance in the algorithm used, the Department answered:

That’s some of what’s involved in the annual reporting requirement, but not the level of detail that you’re asking for.

4.35 Proposed section 29 provides for a review of operation of the Act and provision of identity-matching services to be started within five years of the commencement of the Act. A copy of the report is to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives the report.

4.36 Proposed section 30 provides that the Minister may, by legislative instrument, make rules prescribing matters required or permitted by the Act to be prescribed by the rules or that are necessary or convenient to be prescribed for carrying out or giving effect to the Act. The rules may not do certain things such as create an offence or civil penalty, provide powers of

---

12 Human Rights Law Centre, Submission 16, p. 16.
13 Human Rights Law Centre, Submission 16, p. 21.
14 Mr Andrew Rice, Assistant Secretary, Identity Security Branch, Department of Home Affairs, Committee Hansard, Melbourne, 3 May 2018, p. 29.
15 Mr Andrew Rice, Assistant Secretary, Identity Security Branch, Department of Home Affairs, Committee Hansard, Melbourne, 3 May 2018, p. 29.
arrest or detention; allow for entry, search or seizure, or impose a tax. The rules may not set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in the Act or directly amend the text of the Act.
5. A workable identity-matching regime

5.1 The lack of detail in the IMS Bill has made the Committee’s review challenging. The Bill sets out a minimum framework for a regime that will allow the legal use of the identity-matching-services. The regime is supported by existing agreements and legislation and contemplated agreements and policies. These include the IGA, the Privacy Act 1988 and Participation Agreements and Access Policies.

5.2 However, a citizen should be able to read a piece of legislation and know what that legislation authorises and what rights and responsibilities the citizen has in relation to that legislation. This is especially important in the case of the IMS Bill which has the potential to affect the majority of the Australian population. It is clear that the IMS Bill does not inform the citizen reader in this way.

5.3 Likewise, the lack of detail in the Bill was a problem for submitters. Many resorted to broad analysis of the Bill and, although submitters suggested amendments where they could, submitters usually outlined broad principles that the IMS Bill should address.

5.4 Whilst the Committee supports the aims of the IMS Bill, the Bill would need a significant amount of re-drafting and not simple amending to be in a positon where the Committee could fully support the Bill itself.
5.5 It is not the Committee’s role to re-draft bills. However, to assist in this re-drafting the Committee has decided to outline a set of broad principles supported by more detailed findings in relation to the IMS Bill. These principles are:

- the regime should be built around privacy and transparency,
- the regime should be subject to Parliamentary oversight and reasonable, proportionate and transparent functionality, and
- the regime should be one that requires reporting on the use of the identity-matching services.

5.6 These principles and finding should be used as a template for the re-drafting of the Bill but should not be considered an exhaustive listing of the serious issues the Committee has with the Bill.

**Recommendation 1**

5.7 The Committee recommends that the Identity-matching Services Bill 2019 be re-drafted taking into account the following principles:

- the regime should be built around privacy, transparency and subject to robust safeguards,

- the regime should be subject to Parliamentary oversight and reasonable, proportionate and transparent functionality,

- the regime should be one that requires annual reporting on the use of the identity-matching services, and

- the primary legislation should specifically require that there is a Participation Agreement that sets out the obligations of all parties participating in the identity-matching services in detail.

The Identity-matching Services Bill 2019 should be re-drafted taking into account the Committee’s findings in this report. The Committee notes that the findings alone do not set out all of the matters that would bring the Identity-matching Services Bill 2019 into line with the principles outlined above.
Recommendation 2

5.8 The Committee recommends that, following implementation of recommendation one of this report and subsequent re-introduction to the House, the Identity-matching Services Bill 2019 be referred to the Committee for further review.

5.9 Discussion of the broad principles, findings and Committee comment on matters of importance follow.

Biometric systems and privacy

5.10 The IMS Bill is the enabling legislation for a new scheme that could permit all levels of government and the private sector unprecedented access to Australian citizens’ private biometric information in the form of a facial image. This access could also be extended to any other type of biometric data. Given the significance of these measures, the Committee considers it preferable that privacy oversight and safeguards are established and set out in this enabling legislation rather than only being provided in supplementary agreements or arrangements.

5.11 The Committee accepts that it is not the Government’s intent to set up the identity-matching services scheme without privacy safeguards in place. However, few privacy safeguards are currently set out in the IMS Bill. Rather, they are detailed in the IGA, in the Explanatory Memorandum and in proposed Participation Agreement and Access Policies. None of these materials have the force or protection of legislation. At the time of finalising this report, the Committee had not had access to the proposed Participation Agreement or draft Access Policies to ensure that these deliver the Government’s stated objective.

5.12 The Committee also accepts that the Government relies on privacy protections contained within the Privacy Act 1988 and, where it exists, state and territory privacy legislation. However, these safeguards should be specifically referred to in the IMS Bill. The explicit provision of these safeguards is, in the Committee’s view, necessary to provide community assurance of the protection and maintenance of their private information.

5.13 As noted above, contemplated Participation Agreements and Access Policies will underpin the regime as envisaged in the IMS Bill. The Committee accepts that this is necessary and that, following passage of the IMS Bill, these agreements and policies may take some time to be drafted or revised.
and agreed to by parties. The Committee shares the concern of the Office of the Information Commissioner (Queensland) that instruments that underpin the IMS regime – the Intergovernmental Agreement on Identity Matching Services, Participation, Agreements, Access Policies, the Training Policy, the Compliance Policy, the Charging Policy and Privacy Impact Assessments – run to hundreds of pages, and it may not be realistic to assume that all individual users of IMS will be familiar with the details of these documents. Elevating core intentions, principles and protections into law will help clarify the parameters of the regime, minimise risk of scope creep, and minimise risk of disproportionate privacy incursions.¹

5.14 While the Committee accepts that it is necessary to develop Participation Agreements and Access Policies, the Committee considers that the IMS Bill itself should set out a requirement that the Participation Agreements and Access Policies prescribe (among other things) the roles, rights and minimum obligations of agencies and organisations in relation to their use of identity-matching services. Necessarily, the terms of any Participation Agreement or Access Policy would have to be consistent with the roles, rights and minimum obligations prescribed by the Bill.

5.15 Accordingly, the Committee expects that, to ensure transparency, the underlying broad principles of these agreements should be set out in the Bill.

Principle 1 – a regime built around privacy and transparency

5.16 It should be a principle of the IMS Bill that the Bill itself:

- explicitly sets out a requirement that the Participation Agreements and Access Policies prescribe the roles, rights and minimum obligations of all agencies and organisations in relation to their participation in, access to, and use of, identity-matching services;
- require that the terms of any Participation Agreement or Access Policy be consistent with the roles, rights and minimum obligations of users set out in the Bill;
- expressly provide that State and Territory governments are not precluded from imposing more stringent access requirements to identity-matching services by State and Territory enforcement agencies than those set out in the IMS Bill; and
- require that all Participation Agreements and Access Policies be made public.

¹ Office of the Information Commissioner (Queensland), Submission 3, p. 3.
**Privacy protections should be specified in the Bill**

5.17  The Committee finds that the IMS Bill should set out and ensure that Australian Government, State and Territory government and non-government users of the identity-matching services are subject to:

- the *Privacy Act 1988*(Cth) and to the Australian Privacy Principles, where these entities are subject to that Act, or
- for entities that are not subject to the *Privacy Act 1988* (Cth), a written law or agreement providing:
  - protects personal information in accordance with the Australian Privacy Principles,
  - is monitored for compliance, and
  - has 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.

5.18  The Committee notes that South Australia and Western Australia do not have existing privacy legislation. However, given concerns expressed by some submitters in respect of the adequacy of privacy protections in the IMS Bill, the Committee considers that all users of the identity-matching services should be subject to a law or legally enforceable agreement that protects personal information in accordance with the Australian Privacy Principles – even if that means that some State and Territory jurisdictions may have to enact new privacy legislation in order to satisfy such a requirement. As a matter of principle, the IMS Bill should not enable personal information held by an agency in a jurisdiction with strong, legislated privacy safeguards to be shared with an agency in another jurisdiction where such safeguards may not exist.”

**Minimum access requirements should be included in the Bill**

5.19  The Committee also notes that although it is the Government’s intent that access to identity-matching services will be subject to Participation Agreements and Access Policies (as stated in the IGA), the IMS Bill is silent on this matter.

5.20  The Committee therefore finds that the IMS Bill should be amended to clearly state that access to identity-matching services is subject to signature of Participation Agreements and Access Policies. The Committee is of the view that this would provide greater clarity of the Commonwealth’s intent in the development and operation of the interoperability hub and the National Driver Licence Facial Recognition Solution.
5.21 Further, the Committee finds that the IMS Bill should:

- include a requirement that the Participation Agreements set out the roles, rights and minimum obligations of all agencies and organisations in relation to their participation in, access to, and use of, identity-matching services,
- require that the terms of any Participation Agreement or Access Policy be consistent with the roles, rights and minimum obligations of users set out in the Bill,
- expressly provide that State and Territory governments are not precluded from imposing more stringent access requirements to identity-matching services by State and Territory enforcement agencies than those set out in the IMS Bill, and
- require that all Participation Agreements and Access Policies may be made public.

5.22 These amendments would provide greater assurance and clarity to the Australian public that any agency or organisation that uses an identity-matching service must satisfy minimum privacy benchmarks as set out in the primary legislation.

** Appropriately funded oversight**

5.23 In considering whether there should be a separate biometrics commissioner in Australia, the Committee noted evidence from the OAIC that the ‘identification information’ captured by the proposed identity-matching services may be classified as either ‘personal information’ or ‘sensitive information’ under the Privacy Act. The Committee notes that many of the entities who will have access to the proposed identity-matching services come under the remit of the Privacy Act, the APPs and the OAIC.

5.24 The Department of Home Affairs submitted that it does not support the establishment of a new biometrics commissioner on the ground that the IMS Bill ‘is not seeking to expand the circumstances in which police can collect information from individuals, or govern their use or retention of biometric information’. However, the Committee does not think that the National Driver Licence Facial Recognition Solution and the identity-matching services in the IMS Bill should be considered in isolation from existing biometric databases, such as the National Criminal Investigation DNA Database and the National Automated Fingerprint Identification System. In the Committee’s view, the development of new and existing biometric matching services points to the need for a new oversight mechanism. To that
end, the Committee believes that the government should consider the establishment of appropriate oversight to oversee the collection and use of biometric data under Commonwealth legislation. Numerous submitters cited the UK Biometrics Commissioner as a possible model.²

5.25 The particulars of the new oversight mechanism ought to be the subject of consultation – the Committee finds that the OAIC’s resourcing should be reviewed in order to account for any potential increase in workload that oversight of the identity-matching services.

**Notice and consent**

5.26 The Committee notes the evidence from the Department of Home Affairs that issues around consent and notice will be handled by those entities that collect information. The Committee understands the practical limitations to the Department of Home Affairs checking that each and every request by a local government authority or non-government entity for biometric information has adhered to consent and notification requirements. Given those limitations, it is critical that consent and notice requirements are more clearly defined in the IMS Bill. These requirements should extend to all, not just local, government entities.

5.27 The Committee therefore finds that the IMS Bill should include a requirement for the government or non-government entities to provide clear notice to individuals of the collection and use of their identifying information and gain consent for the use of biometric data in the interoperability hub. This would be consistent with the IGA.

5.28 It would be unfeasible for certain agencies (such as security agencies) to have to seek consent and that provisions exist in other Acts which exempt these agencies from consent. The Committee therefore finds that the above requirements should be applied unless there is an exemption, for that entity, under Commonwealth, State or Territory law that removes a requirement for consent.

5.29 Notice provided to individuals should include the following:

- practices undertaken in relation to the face matching services,
- the risks to the individual in the event that their biometric data is compromised,

---

• the absence of any enforceable legal remedy if the information is lost or breached,
• the jurisdiction and control over the data hosting and usage mechanisms, and
• the full list and description of identity-matching systems which may be able to use this data once collected.

5.30 In addition, the Committee recommends that the IMS Bill should make clear that, where an individual does not consent for the use of their biometric data, the local government authority or non-government entity must have an alternative means for checking identity—such as a points check via various forms of identification documents—so that an individual is not disadvantaged when seeking local government authority or non-government entity services.

Publication of the Intergovernmental Agreement

5.31 The Committee notes the central importance of the IGA to the IMS Bill. The IGA provides a significant amount of additional information into how the identity-matching services will operate. That Committee finds that it is important that the IGA always be available for Australian citizens—those affected by the IMS Bill—to access. The Committee therefore finds that:

• the IGA should be publicly accessible at all times (for example, by way of inclusion as a Schedule to the IMS Bill), and
• any future revisions to the IMS Agreement be published on the Council of Australian Governments’ website.

Identity-matching services, the interoperability hub and the National Driver License Facial Recognition Solution

5.32 As mentioned earlier, it is important that appropriate safeguards around identity-matching services are established in this enabling legislation. The Committee notes the potential for a wide range of biometric markers that could be used for identity verification. Biometrics matching is a relatively new technology whose capability and application is growing exponentially. Therefore, proper oversight and reasonable and proportionate functionality must be the basis on which identity-matching services are provided to appropriate government and non-government entities.
Principle 2 – a regime subject to Parliamentary oversight and reasonable, proportionate and transparent functionality

5.33 It should be a principle of the IMS Bill that the regime it creates is subject to Parliamentary oversight and reasonable proportionate and transparent functionality.

New identity information and identity-matching services subject to Parliamentary scrutiny

5.34 Currently, the scope of biometrics proposed to be collected and used for the identity matching services regime proposed in the Bill is limited. However the ministerial rule making powers contained in subsections 5(1)(n) and 7(1)(f) of the Bill mean that a Minister could make rules allowing for any number of the biometric markers, such as iris scanning, to be included as identification information that form part of an identity-matching service.

5.35 The Committee notes the concerns of the AHRC and the Law Council in relation to these powers.

5.36 The Committee also notes that the Department of Home Affairs sought to distinguish the use of rules in the IMS Bill from those discussed by the Committee’s Advisory Report on the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014.

5.37 In light of the evidence that it has considered to date, the Committee does not currently accept that it is appropriate to provide a mechanism for the Minister to add to the definition of identification information or identity-matching services.

5.38 The Committee notes the Law Council of Australia’s concern that clause 5(1)(n) could provide an opportunity for a future Minister to enhance the scope of the identity-matching scheme without the need for primary legislation. The Committee also notes the concern of the Victorian Government that, by giving the Minister the rule-making powers that are currently proposed, the IMS Bill provides scope for going beyond what was agreed in the Intergovernmental Agreement on Identity Matching Services. It is possible that, because of this, a situation may arise where the Commonwealth is authorised to collect information as
part of the IMS that Victoria is not authorised to disclose under its legislation or otherwise.³

5.39 In light of those considerations, the Committee agrees with the Law Council (among others) that clause 5(1)(n) should be deleted so that the definition of identification information can only be amended by primary legislation.

5.40 While the Committee accepts that the government does not intend to use the identity-matching services to carry out ‘many-to-many’ or ‘many-to-one’ checks, the Committee also shares the concern of the Office of the Information Commissioner (Queensland) that the power in clause 7(1)(f) could theoretically empower the Minister to allow for this. In the absence of a compelling justification that such a rule-making power is necessary (as opposed to expedient), the Committee considers that clause 7(1)(f) should also be deleted.

5.41 However, the Committee notes that the Government will have a further opportunity to provide the Committee with a compelling justification if it maintains that a rule-making power is necessary in this context.

5.42 The Committee notes that the deletion of the rule-making powers in clauses 5(1)(n) and 7(1)(f) would ensure any proposal to add to the definition of identification information or identity-matching services is adequately scrutinised, provide proper public assurances and ensure appropriate privacy safeguards are in place.

Reasonable and proportionate functionality

The potential for mass or blanket surveillance

5.43 The Committee also considered the concerns raised regarding the potential for using mass or blanket surveillance, such as Close Circuit Television (CCTV), for individual identification. The Committee accepts that this use of identity matching services is not intended in the Bill.

5.44 The Committee notes concerns raised throughout the review regarding the activities of ‘gathering intelligence’, ‘verifying the identity of individuals’ and ‘road safety’ and that these activities should not be authorised by the IMS Bill.

³ Victorian Government, Submission 14, p. 3.
5.45 The Committee notes that these activities are part of those envisioned by the IGA and, where identity-matching services are used for activities, including verifying identity, by local government authorities or non-government entities, this will only be able to be done with the consent of the individual (see subclause 7(3)).

The inclusion of gathering intelligence, road safety and identity verification activities

5.46 Based on the additional privacy and safeguards against misuse included in findings by the Committee in this report, the Committee accepts – in principle – the inclusion of the intelligence gathering, road safety and identity verification activities contemplated by the IMS Bill.

A more proportionate definition of national security

5.47 The Committee notes that proposed section 6(4) of the IMS Bill defines the term ‘national security’ by reference to the National Security Information (Criminal and Civil Proceedings) Act 2004. This is a broad definition designed to be interpreted by a sitting judge in circumstances where evidence that may have a national security aspect is being, or is contemplated being, submitted in court. Since the introduction of the IMS Bill to Parliament the passage of the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 has inserted a new section 90.4 into the Criminal Code which provides a more constrained definition of ‘national security’.

5.48 A constrained definition of national security is more appropriate and proportionate in circumstances where government action, such as the use of the identity-matching services, is contemplated. The Committee notes that the Department of Home Affairs offered no objection to this definition being used. The Committee therefore finds that the IMS Bill should be amended so that the definition of ‘national security’ in section 6(4) refers to section 90.4 of the Criminal Code Act 1995.

Appropriately defining the functionality of the identity-matching services

5.49 The Committee shares the concerns of submitters that the functionality of each of the identity-matching services may be included in the IGA, but are not appropriately defined in the IMS Bill itself. The Committee therefore finds that the IMS Bill should be amended to more fully define the operation

---

4 Criminal Code Act 1995, section 90.4.
and functionality of each of the identity-matching services. Such a definition should encompass:

- the purpose of the service,
- the technology used by the service (e.g., which biometric indicators), and
- the functionality of the service.

5.50 It is the Committee’s view that the use of the Face Verification Service by a non-government entity must only return a “match or no match” response.

The Face Identification Service

5.51 The Committee notes the Facial Recognition Service, Face Verification Service, Identity Data Sharing Service and the One Licence Service raised fewer concerns with submitters. These services are generally used to match biometric data for the purposes for which it was collected. The main concerns with these services as proposed in the Bill were in relation to the text of the IMS Bill not according with the intent of the text of the IGA. In addition, the Committee notes the general concern that, in relation to any use of the identity-matching services, the minimum amount of data needed should be returned and, in relation to the Face Verification Service, the Committee notes concerns that data linked to a verified identity could be on sold.

5.52 The Committee’s findings of increased privacy safeguards, referencing Access and Participation agreements in the IMS Bill, and more adequately defining the functionality of each of the identity-matching services, should alleviate many of these general concerns.

5.53 The Committee notes that the majority of specific concerns were in relation to the Face Identification Service.

5.54 The Committee notes that the Face Identification Service is a one-to-many rather than a one-to-one matching system. It is a system that, in addition to the biometric data of a potential suspect in a crime, necessarily makes use of the biometric data of a number of wholly innocent people. As such, the Face Identification Service could be considered a more significant imposition on the privacy of many Australian citizens.

5.55 The Committee notes the tension between the rights of Australian citizens to their privacy and the pressures facing law enforcement when investigating crime.

5.56 However, the Committee has not been persuaded that it would be inappropriate to require an enforcement agency to obtain a warrant in order
to access the Face Identification Service, and therefore requests further advice and briefings from relevant enforcement and security agencies.

5.57 The Department of Home Affairs argued against the need for a warrant. In doing so, the Department cited the Attorney-General’s Department *Guide to Framing the Commonwealth Offences, Infringement Notices and Enforcement Powers of 2011* which sets out when it is appropriate to require agencies to obtain a warrant. One such circumstance is where there is entry to premises without consent.

5.58 In this context, the Committee notes the statement made by Mr John Howell, from the Australian Human Rights Commission, which argues that ‘warrant regimes can be designed, and in fact currently are designed and operated, to allow for warrants to be obtained very quickly in emergency situations and outside business hours overnight. That is quite possible and feasible, and in fact occurs.’

5.59 The Committee notes concerns with respect to the power contained in section 8(2)(q) to allow the Minister to give an additional entity the ability to request the provision of the Face Identification Service.

5.60 The Committee notes that this power is intended only to be used following a machinery of government, name or legislative change, without having to amend the Act. The Committee further notes that the IMS Bill provides that, before the Minister makes rules prescribing access to the Face Identification Service, 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 in proposed section 8(2).

5.61 However the Committee considers that access to biometric data amounts to a significant intrusion into privacy and as such requires significant safeguards.

5.62 The Committee notes the concerns of submitters in respect of the Minister’s discretion to allow an agency to request access to the Face Identification Service. In particular, while the Minister is required to have regard to certain

---


matters, his or her discretion to allow an agency to request access to the Face Identification Service is not otherwise fettered on the face of the legislation.

5.63 The Committee notes the concerns of some submitters in respect of the power contained in section 8(2)(q) to allow the Minister to give an additional entity the ability to request the provision of the Face Identification Service. In the Explanatory Memorandum for the IMS Bill, the Minister stated that the power in clause 8(2)(q) is ‘solely intended’ to allow the agencies listed in clause 8(2) to continue to use the Facial Identification Service ‘following a machinery of government, name or legislative change without having to amend the Act’.

5.64 In view of the limited circumstances in which it is intended to be exercised, and having regard to the concerns expressed by submitters, the Committee considers that clause 8(2)(q) should be deleted. There should be no ‘urgent circumstances’ that would warrant an exercise of the ministerial power in clause 8(2)(q). If there is a ‘machinery of government’ legislative amendment, it is the Committee’s view that clause 8(2) ought to be amended by primary legislation at the same time.”

5.65 Further, consistent with the existing provisions of the Bill, the Minister must have regard to the factors listed in proposed section 8(3).

5.66 The Committee took specific note of the evidence given that the scope of use of the identity-matching services in relation to general law enforcement is different to that contained in the IGA. The Committee also notes the Department of Home Affairs’ inconsistent evidence on this matter.

5.67 In relation to general law enforcement, the IGA provides for:

- the prevention, detection, investigation or prosecution of an offence under Commonwealth, state and/or territory laws carrying a maximum penalty of not less than three years imprisonment, and
- for use by agencies within the same jurisdiction for law enforcement purposes in relation to offences with penalties of less than three years.

5.68 This distinction between cross and intra jurisdictional general law enforcement of the Face Identification Service is not reflected in the IMS Bill. The Committee finds that the IMS Bill should be amended so that general law enforcement access to the Face Identification Service is only permitted for the cross jurisdictional prevention, detection, investigation or prosecution of an offence that carries a maximum sentence of not less than three years imprisonment in the jurisdiction in which it is being investigated.
Reasonable and proportionate use of the results of identity-matching information

5.69 In addition to privacy, the Committee notes concerns regarding the weight given to identity matching results in judicial proceedings. The IGA outlines that it is not intended that results from identity-matching services would be used as the sole basis for ascertaining an individual’s identity for evidentiary purposes. The Committee notes that this is not currently clearly established in the IMS Bill and finds that it should be set out clearly in the IMS Bill.

Collection, use, protection and disclosure of identification information and reporting, and review requirements

5.70 Clause 19 of the IMS Bill, provides that:

- if a law of a State or Territory limits disclosure of some or all identification information by an authority of that State or Territory; but
- exempts from that limitation a disclosure authorised by a Commonwealth law,
- the relevant authority body or person may disclose to the Department identification information for inclusion in the NDLFRS.

5.71 The Committee finds that this clause should be deleted.

5.72 The Minister has explained that this is an expediency measure ‘to reduce the number of states and territories that would need to amend their own legislation before Home Affairs could develop the database’.

5.73 However, the inclusion of this provision in the Bill is inconsistent with the Intergovernmental Agreement on Identity Matching Services, which provides that legislation enacted in state and territory jurisdictions should authorise states and territories to provide facial images and related identity information to the host of the NDLFRS.

5.74 As the state and territory authorities are currently entrusted with safeguarding the identification information that they hold, it should be a matter for state and territory parliaments to expressly authorise the disclosure of that information for the purpose of developing the NDLFRS or making that information available for the purposes of an identity-matching service.

---

7 IMS Bill, Explanatory Memorandum, p. 31.
8 COAG, Intergovernmental Agreement on Identity Matching Services, 5 October 2017, p. 20.
5.75 As well as being consistent with the Intergovernmental Agreement on Identity Matching Services, this amendment will serve to build public confidence in the NDLFRS and the identity matching services it facilitates, and give them greater democratic legitimacy.

5.76 The Committee received limited evidence in relation to proposed sections 26-30 of the Bill which provide for the delegation of the Secretary’s powers, annual reporting and review of the IMS Bill. However, it is the Committee’s view that clause 29 should be amended to require the Minister to cause a review of the operation of the Act and the provision of identity-matching services within two years of the Act’s commencement.

5.77 Although there was a lack of submitted evidence on the topic, the Committee considers that reporting on the use of the identity-matching services is an oversight requirement equally as important as those sections of the IMS Bill that received more attention.

**Principle 3 – a regime that requires reporting on the use of the identity-matching services**

5.78 It should be a principle of the IMS Bill that the regime it creates requires reporting on the use of the identity-matching services.

**ASIO statistics**

5.79 The Committee has considered the exemption provided to ASIO in relation to exceptions to public statistics reporting under proposed sections 28(1)(a) and (c). Given the sensitive nature of ASIO’s work, the Committee is satisfied that such an exemption is appropriate.

5.80 The Committee also notes ASIO’s annual reporting requirements as outlined in section 94 of the *Australian Security Intelligence Organisation Act 1979* and finds that it is important and appropriate that ASIO include in its classified annual report statistics reporting as envisioned under proposed sections 28(1)(a) and (c) of the IMS Bill.

**Annual reporting**

5.81 The Committee also notes that the Minister has agreed to seek to amend the IMS Bill to provide for annual reporting in relation to the number of instances in which an entrusted person discloses protected information to lessen or prevent a threat to life or health as provided for in section 23 of the IMS Bill.
5.82 The Committee notes the commercial confidentiality concerns raised by the Department in relation to private sector users of the identity-matching services. No further detail was provided to the Committee in relation to these concerns. The Committee notes that the general public, by consenting to the use of identity-matching services, will become aware of private sector users of identity-matching services. The Committee is therefore satisfied and finds that this information should be provided in the annual report.

5.83 The Committee notes evidence from the Human Rights Law Centre that it is possible to capture and analyse accuracy rates of facial recognition algorithms. Annual reporting of such accuracy rates will serve to give the Australian public confidence in the identity-matching services envisaged by the IMS Bill.

5.84 The Committee notes the suggestion that reporting requirements in relation to data breaches could be characterised as a ‘double up’. The Committee considers that, given the intrusive nature of the identity-matching services, people should expect that data breaches in relation to those services, even if reported elsewhere, should be included in an annual report specifically dealing with the identity-matching services.

5.85 In relation to security incidents, such as unauthorised access or unauthorised disclosure of identification information, the Committee is not convinced that providing statistical information on such incidents will create a security risk. The Committee notes the Department of Home Affairs’ evidence that this information will be captured and, therefore, should be easily reportable.

5.86 The Committee therefore finds that the following should also be included in the annual report required under proposed section 28 of the IMS Bill:

- the number of instances in which an entrusted person discloses protected information to lessen or prevent a threat to life or health,
- the names of private sector users of the Facial Verification Service,
- the accuracy rates of the biometric facial recognition algorithms used by the identity-matching services,
- any data breaches notified under the provisions in Part IIIC of the Privacy Act 1988, and
- any security incidents in relation to use of the identity-matching services.
Update reporting on all Participation Agreements and Access Policies and their compliance

5.87 The Committee notes that much of the detail on the implementation of the IMS Bill will be contained in Participation Agreements and Access Policies under which specific conditions can be placed on use of a particular agency’s data by another entity.

5.88 Whilst the Committee accepts that these detailed agreements are not all currently available it finds that, one year after Royal Assent of the IMS Bill, the Department of Home Affairs should provide the Committee with a written update report on all Participation Agreements and Access Policies and their compliance. The Department of Home Affairs should also be available to provide the Parliamentary Joint Committee on Intelligence and Security with a briefing on this report.
6. Australian Passports Amendment (Identity-matching Services) Bill 2019

6.1 The Australian Passports Amendment (Identity-matching Services) Bill 2019 (the Passports Amendment Bill) seeks to amend the Australian Passports Act 2005 to authorise the Minister for Foreign Affairs to disclose personal Australian travel document data for the purpose of participating in the identity-matching services, as agreed by COAG in the intergovernmental agreement.

6.2 Proposed section 1 of the Passports Amendment Bill inserts, after section 46(d) of the Australian Passports Act 2005, a new section 46(da) allowing that the Minister may disclose personal information for the purpose of participating in a service, specified or of a kind specified in the Minister’s determination, to share or match information relating to the identity of a person.

6.3 By making such a determination, the Minister will be able to authorise the disclosure of personal information via an identity-matching service for all
the purposes of that service, rather than just for purposes already set out in other parts of section 46 or in other legislation, such as the Privacy Act 1988.¹

6.4 Proposed section 2 of the Passports Amendment Bill has the effect that the Minister will be able to authorise the disclosure of any relevant personal information that the Department has on record, not just information collected after the commencement of the item.²

6.5 Proposed section 3 of the Passports Amendment Bill inserts, after section 56 of the Australian Passports Act 2005, a provision allowing that the Minister may arrange for the use, under the Minister’s control, of computer programs for any purposes for which the Minister may, or must, make a decision; exercise any power or comply with any obligation; or do anything else related to making a decision or exercising a power or complying with an obligation.

6.6 In addition, the Minister may make a decision in substitution if the Minister is satisfied that the decision made by the operation of the computer program is incorrect.

6.7 The Explanatory Memorandum points out that the intended decisions will be low-risk decisions that a computer can make within objective parameters. Examples of such decisions are decisions to collect personal information for processing passport applications using the Face Verification Service, and decisions to issue passports to people whose biographical data and facial images match previous passport applications.³

**Delegated legislation**

6.8 In relation to the proposed section 46(da) expanding the Minister’s rule making powers to disclose information for particular purposes, the joint councils for civil liberties stated that rules ‘which have a significant impact on individual rights and liberties should be included in the primary legislation’ and that by leaving these decisions to ‘delegated legislation and

---

¹ Australian Passports Amendment (Identity-matching Services) Bill 2019 (Passports Amendment Bill), Explanatory Memorandum, p. 8.

² Passports Amendment Bill, Explanatory Memorandum, p. 8.

³ Passports Amendment Bill, Explanatory Memorandum, pp. 8-9.
eliminating barriers to data sharing, the level of scrutiny of these processes is reduced’.⁴

6.9 The joint councils recommended that proposed section 46(da) be ‘amended to specify that provisions impacting individual rights and liberties should be included in the Act, not in rules determined outside the legislation’.⁵

6.10 In relation to the concerns raised by the joint councils, the Department of Foreign Affairs and Trade (DFAT) explained that ‘the Determination is a transparent and publically available instrument. Amendments to the Determination are tabled in Parliament for a disallowable period’.⁶

**Automated decision-making**

6.11 A number of submitters raised concerns around automated decision-making. The Australian Lawyers for Human Rights (ALHR) considered that ‘Section 56A is overbroad’, ‘does not distinguish discretions from other decisions’ and does not ‘provide for a hearing in appropriate circumstances, or specify how a decision can be challenged in case of error’.⁷

6.12 Submitters raised specific concerns around the fallibility of automated decision-making. The joint councils for civil liberties argued that incorrect or unfair decisions and lack of procedural fairness are a danger when computers replace a human decision maker.⁸

6.13 Similarly, the ALHR pointed to the possibility that ‘the computer programme might come to the wrong conclusion and that the Minister might need to reverse the programme’s decision.’ This, the ALHR argued, makes it clear that ‘the legislation itself acknowledges the fallibility of a computer programme’.⁹

6.14 Given this possibility for fallibility, Civil Liberties Australia suggested that the Bill should be amended so that individuals ‘always have the right to

⁶ Department of Foreign Affairs and Trade, *Submission 15*, p. 10.
request a human make a decision that affects their legal rights and obligations’.\(^\text{10}\)

6.15 DFAT explained that acknowledgement by the Passports Amendment Bill that automated decision-making can make an error is included to make clear, and for the avoidance of doubt, ‘that the Minister is able to substitute incorrect automated decisions made in favour of a client’.\(^\text{11}\)

6.16 In answer to the broad concerns around automated decision-making, DFAT stated that these concerns are ‘based on an expectation that the Department intends to use automation to make decisions that may have a negative impact on the subjects of those decisions. This is not the case’.\(^\text{12}\)

6.17 Additionally DFAT stated that given the way that the [Face Verification Service], the [Face Identity Service] and the Department’s passport processing systems are designed, the Department is in practice only able to automate decisions that produce favourable or neutral outcomes for the subject. Such decisions would not negatively affect a person’s legal rights or obligations, and would thus not generate a reason to seek review.\(^\text{13}\)

**Committee comment**

6.18 The Committee notes that, in comparison to the evidence it received on the Identity-matching Services (IMS) Bill 2019, there were few issues raised in relation to the Passports Amendment Bill.

6.19 The Committee notes the concerns in relation to delegated legislation. The Committee has made recommendations in relation to delegated legislation contained within the IMS Bill. However, the Committee does not recommend that the Minister’s powers in proposed section 46(da) should be amended. The services that the Minister may determine participation in are limited and subject to parliamentary oversight by virtue of the Committee’s proposed amendments to the IMS Bill.

6.20 Whilst the Committee notes the concerns around automated decision making, the Department has stated that such decisions can only be made

\(^{10}\) Civil Liberties Australia, *Submission 5*, p. 3.

\(^{11}\) Department of Foreign Affairs and Trade, *Submission 15*, p. 9.

\(^{12}\) Department of Foreign Affairs and Trade, *Submission 15*, p. 9.

\(^{13}\) Department of Foreign Affairs and Trade, *Submission 15*, p. 9.
when they produce favourable or neutral outcomes for the subject. However, the Committee also notes that this is not reflected in the text of the Passports Amendment Bill or the Explanatory Memorandum. The Committee recommends that this be made clear in the Passports Amendment Bill.

**Recommendation 3**

6.21 The Committee recommends that the Australian Passports Amendment (Identity-matching Services) Bill 2019 be amended to ensure that automated decision making can only be used for decisions that produce favourable or neutral outcomes for the subject, and that such decisions would not negatively affect a person’s legal rights or obligations, and would not generate a reason to seek review.

**Concluding comments**

6.22 The Committee notes that the Passports Amendment Bill ensures that there will be a clear legal basis for DFAT to participate fully in the identity-matching services. The Committee further notes that amendments made to the IMS Bill may have consequential effects on the Passports Amendment Bill and recommends that, following the implementation of Recommendation 3, the Passports Amendment Bill not proceed until Committee has completed its review of the revised version of the Identity-matching Services Bill 2019 (as anticipated by Recommendation 2). If, as a consequence of amendments made to the IMS Bill, further amendments are made to the Passports Amendment Bill, the Passports Amendment Bill should, in accordance with Recommendation 2, also be referred to the Committee for further review.

**Recommendation 4**

6.23 The Committee recommends that, following the implementation of Recommendation 3, the Passports Amendment Bill not proceed until the Committee has completed its review of the revised version of the Identity-matching Services Bill 2019 (as anticipated by Recommendation 2). If, as a consequence of amendments made to the IMS Bill, further amendments are made to the Passports Amendment Bill, the Passports Amendment Bill should, in accordance with Recommendation 2, also be referred to the Committee for further review.
Mr Andrew Hastie MP

Chair
A. List of submissions

1. Future Wise and the Australian Privacy Foundation
2. Australian Lawyers for Human Rights
3. Office of the Information Commissioner (Queensland)
4. Office of the Victorian Information Commissioner
5. Civil Liberties Australia
6. Australian Security Industry Association Limited
   - 6.1 Supplementary to submission 6
7. Tasmanian Government
8. Law Council of Australia
   - 8.1 Supplementary to submission 8
   - 8.2 Supplementary to submission 8
9. Joint councils for civil liberties
   - 9.1 Supplementary to submission 9
10. Queensland Council for Civil Liberties
11. Australian Human Rights Commission
   - 11.1 Supplementary to submission 11
   - 11.2 Supplementary to submission 11
12. Department of Home Affairs
12.1 Supplementary to submission 12
12.2 Supplementary to submission 12
12.3 Supplementary to submission 12
12.4 Supplementary to submission 12

13 Office of the Australian Information Commissioner

14 The Victorian Government

15 Department of Foreign Affairs and Trade
   - 15.1 Supplementary to submission 15

16 Human Rights Law Centre
   - 16.1 Supplementary to submission 16
   - 16.2 Supplementary to submission 16

17 Dr Marcus Smith
   - 17.1 Supplementary to submission 17

18 Fergus Hanson, Australian Strategic Policy Institute
   - 18.1 Supplementary to submission 18

19 Dr Paul Henman

20 Professor Liz Campbell

21 Paul Sharp

22 Ash White

23 Zac Ford

24 Robert Sweet

25 Maria Casamento

26 Australian Mobile Telecommunications Association

27 Allens Hub for Technology, Law and Innovation at UNSW Law

28 Optus

29 Sue-Ellen Middleton

30 Rebecca King

31 Tanja Price

32 Lyn Craven

33 Robert Bury
34 Sophie Novasari
35 Connie Crawford
36 Robyn Reynolds
37 Digital Transformation Agency (DTA)
38 Department of Human Services
39 Australian Security Intelligence Organisation
   • 39.1 Supplementary to submission 39
40 Electronic Frontiers Australia
B. List of witnesses appearing at the public hearings

Thursday, 3 May 2018

St Andrews Place, East Melbourne

*Australian Human Rights Commission*

- Mr Edward Santow, Human Rights Commissioner
- Mr John Howell, Director, Human Rights Scrutiny

*Law Council of Australia*

- Mr Morry Bailes, President
- Dr Natasha Molt, Deputy Director of Policy
- Ms Olga Ganopolsky, Chair, Privacy Law Committee of the Business Law Section
- Mr Peter Leonard, Member, Media and Communications Committee of the Business Law Section.
Department of Home Affairs

- Ms Maria Fernandez, Deputy Secretary Intelligence and Capability Group
- Mr Andrew Rice, Assistant Secretary, Identity Security Branch
- Mr Steve McGlynn, Assistant Secretary, National Security and Law Enforcement Legal Branch

Department of Foreign Affairs and Trade

- Mr Guy O’Brien, Corporate Counsel
- Mr Stephen Gee, Assistant Secretary – Passport Policy and Integrity Branch

Friday, 17 August 2018

Parliament House, Canberra

Human Rights Law Centre

- Mr Hugh de Kretser, Executive Director

Australian Strategic Policy Institute

- Mr Fergus Hanson

Department of Home Affairs

- Mr Andrew Rice, Assistant Secretary, Identity Security Branch
- Mr Stephen Webber, Assistant Secretary, National Security & Law Enforcement Legal Branch
- Mr Duncan Anderson, Acting Assistant Secretary, Identity Security Branch