PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

PARLIAMENTARY LIBRARY
INFORMATION ANALYSIS ADVICE

BILLS DIGEST

BILLS DIGEST NO. 21, 2019–20 26 AUGUST 2019

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

Claire Petrie
Law and Bills Digest Section

Contents

The Bills Digest at a glance 3
Purpose of the Bills 3
How the IMS Bill works 3
Key issues 3
History of the Bill 5
Purpose of the Bill 5
Structure of the Bill 5
Background 6
Biometrics and identity-matching 6
Facial recognition technologies 6
Identity crime in Australia 8
Identity crime and national security 9
National Identity Security Strategy 10
Document Verification Service 11
National Facial Biometric Matching Capability 12
Intergovernmental agreement 13
State and territory legislation 14
Privacy and data security 15
Biometric data and privacy concerns 15
Privacy Act and biometric data 16
Notifiable data breaches scheme 17
Privacy impact assessments 17
Committee consideration 18
Parliamentary Joint Committee on Intelligence and Security 18
Senate Standing Committee for the Scrutiny of Bills 18

Date introduced: 31 July 2019

House: House of Representatives

Portfolio: Home Affairs and Foreign Affairs and Trade

Commencement: Both Bills commence the day after Royal Assent.

Links: The links to the Bills, their Explanatory Memorandum and second reading speech can be found on the Bill's home page for the Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019, or through the Australian Parliament website.

When Bills have been passed and have received Royal Assent, they become Acts, which can be found at the Federal Register of Legislation website.

All hyperlinks in this Bills Digest are correct as at August 2019.

ISSN 1328-8091

Policy position of non-government parties/independents 19
Position of major interest groups 20
Financial implications 22
Statement of Compatibility with Human Rights 22
Parliamentary Joint Committee on Human Rights ... 22
Key issues and provisions 23
How does the system work? 23
Identity-matching facilities 23
Identity-matching services 25
Minister's power to prescribe additional services 25
What information may be shared? 26
Identification information 26
What are the limitations on access? 27
Face Verification Service—access policy 28
Authorisations 28
Identity or community protection activity 29
Face identification service (FIS) 30
Private sector access 31
Restrictions under the Bill 31
Restrictions under the IGA 32
What protections are in place? 33
Disclosure offence 33
When will disclosure be authorised? 34
Minister's rule-making power and the obligation to consult 34
Annual reporting requirement 35
Statutory review 37
Passports Bill 38
Identity-matching capability 38
Computerised decision-making 38

The Bills Digest at a glance

Purpose of the Bills

- The Identity-matching Services Bill 2019 (IMS Bill) authorises the Department of Home Affairs (DOHA) to create and maintain facilities for the sharing of facial images and other identity information between government agencies, and in some cases, private organisations.
- It provides a legislative basis for certain measures contained in the *Intergovernmental Agreement on Identity Matching Services* (IGA), agreed to by COAG leaders on 5 October 2017. This agreement aims to facilitate the 'secure, automated and accountable' exchange of identity information to help prevent identity crime and promote a range of law enforcement, community safety and service delivery objectives.
- The Australian Passports Amendment (Identity-matching Services) Bill 2019 (Passports 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.
- Both Bills were introduced in the same form during the 45th Parliament, but were not debated before the dissolution of the House of Representatives in April 2019.

How the IMS Bill works

- The IMS Bill authorises DOHA 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 agencies and organisations can request and transmit information and
  - the National Driver Licence Facial Recognition Service (NDLRFS), a federated database of information contained in government identity documents such as driver licences.
- The Bill specifies identity-matching services which will operate through the hub. This includes the Face Verification Service (FVS), which allows users to verify a specific person's identity, and the Face Identification Service (FIS), which involves the electronic matching of a facial image with the images of one or more people, in order to identify a person. Private sector entities and local government authorities may have access to the FVS.
- The Bill does not authorise certain agencies to use identity-matching services—entities seeking access will need a legal basis for collecting and disclosing personal information, and must meet access requirements set out in the IGA.
- The Bill creates an offence for entrusted persons to record or disclose protected information in connection with these services, and sets out circumstances where disclosure will be authorised.
- The Minister for Home Affairs will be required to report annually to Parliament about the use of the services. A statutory review is to be started within five years of the Act's commencement.

Key issues

- The Bills are currently being reviewed by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The Committee previously commenced an inquiry into the 2018 versions of the Bills, but the inquiry lapsed at the dissolution of the House of Representatives in April 2019.
- In relation to the 2018 Bills, the Parliamentary Joint Committee for Human Rights, Senate Standing Committee for the Scrutiny of Bills and submissions to the PJCIS inquiry raised concerns that the broad scope of the IMS Bill may enable substantial infringements on privacy rights, allowing disclosure of personal information for an extremely wide range of purposes.
- Stakeholders suggested the IMS Bill provides inadequate protection against misuse of this information, and queried why it does not include key safeguards contained in the IGA, such as access criteria and limitations on the amount of information released by the identity-matching systems.

- Another area of concern is private sector access, with submissions questioning whether this is appropriate, and arguing that there are insufficient safeguards in the Bill at present.
- Stakeholders also raised concerns with the computerised decision-making provision in the Passports Bill, suggesting that it is too broad and should be refined.

History of the Bill

The Identity-matching Services Bill 2018 (IMS Bill 2018) and Australian Passports Amendment (Identity-matching Services) Bill 2018 (Passports Bill 2018) were introduced into the House of Representatives on 7 February 2018. They were not debated, and lapsed at the dissolution of the 45th Parliament on 11 April 2019.[1]

The present Bills were introduced into the House of Representatives on 31 July 2019, and are in the same terms as the 2018 Bills.

A Bills digest was prepared in respect of the 2018 Bills.[2] Much of the material in the present Digest has been sourced from that earlier one.

Purpose of the Bill

The purpose of the Identity-matching Services Bill 2019 (IMS Bill) is to authorise the Commonwealth to facilitate the sharing of identification information, including facial images, between the Commonwealth, states and territories for the purposes of identity-matching. The Bill provides a legal basis for certain aspects of the *Intergovernmental Agreement on Identity Matching Services*, signed by Council of Australian Governments (COAG) leaders on 5 October 2017. The Agreement provides for sharing and matching of identity information to 'prevent identity crime, support law enforcement, uphold national security, promote road safety, enhance community safety and improve service delivery'.[3]

The purpose of the Australian Passports Amendment (Identity-matching Services) Bill 2019 (Passports Bill) is to amend the *Australian Passports Act 2005* (*Passports Act*) to enable the Department of Foreign Affairs and Trade (DFAT) to disclose information for the purpose of participating in identity-matching services, and to authorise the use of computer programs to make decisions.

Structure of the Bill

The IMS Bill has five Parts:

- Part 1 contains a simplified outline of the Act and sets out definitions
- Part 2 authorises the development and operation of identity-matching facilities
- Part 3 authorises the collection, use and disclosure of information by the Department of Home Affairs (DOHA)
- Part 4 contains a disclosure offence and sets out exceptions to this
- Part 5 contains miscellaneous provisions relating to delegation, reporting, review of the operation of the Act and the Minister's rule-making powers.

The Passports Bill has one Schedule, which expands the circumstances in which the Minister for Foreign Affairs and Trade may disclose information and allows the Minister to arrange for the use of computer programs to make decisions.

---

1. Parliament of Australia, 'Identity-matching Services Bill 2018 homepage', Australian Parliament website; Parliament of Australia, 'Australian Passports Amendment (Identity-matching Services) Bill 2018 homepage', Australian Parliament website.
2. C Petrie, *Identity-matching Services Bill 2018 and Australian Passports Amendment (Identity-matching Services) Bill 2018*, Bills digest, 110, 2017–18, Parliamentary Library, Canberra, 22 May 2018.
3. Council of Australian Governments (COAG), *Intergovernmental Agreement on Identity Matching Services*, COAG meeting, Canberra, 5 October 2017.

Background

Biometrics and identity-matching

The collection and use of biometric information is becoming increasingly prevalent in government agencies and the private sector. Biometric information can be understood as information about unique biological or behavioural characteristics which can be used to identify an individual.[4] Biometric identifiers can include 'physiological' identifiers such as fingerprints and palm prints, iris/retinal scans and facial images, as well as 'behavioural' identifiers such as gait and voice.[5]

Although biometric technologies have long existed, the use of biometrics is increasing as advances in technology allow a person's biometric data to be easily collected and matched against existing data-sets, to establish or verify their identity and allow law enforcement authorities to identify individuals of concern.[6]

Facial recognition technologies

The IMS Bill helps to establish a framework for the automated sharing of biometric data—particularly facial images—between federal, state and territory government agencies (and in some cases, local government and private sector organisations). While this sharing is already occurring to some extent, the Explanatory Memorandum provides:

> Current image-based methods of identifying an unknown person can also be slow, difficult to audit, and often involve manual tasking between requesting agencies and data holding agencies, sometimes taking several days or longer to process.[7]

In contrast, the identity-matching services provided for in the Bill enable the rapid, automated sharing and matching of images held in existing government databases, including driver licence, passport and visa photographs. Law academics Monique Mann and Marcus Smith provide the following explanation of how automated facial recognition technology (AFRT) works:

> Traditional forensic facial mapping involves comparing measurements between facial features […] or the similarities and differences in facial features […]. In comparison with these techniques, AFRT involves the automated extraction, digitisation and comparison of the spatial and geometric distribution of facial features. Using an algorithm similar to the ones used in fingerprint recognition, AFRT compares an image of a face with one stored in a database. At the enrolment stage, a digital photograph of a subject's face is taken and a contour map of the position of facial features is converted into a digital template using an algorithm. AFRT systems digitise, store and compare facial templates that measure the relative position of facial features.[8] (References omitted)

---

4. Attorney-General's Department (AGD), *National identity proofing guidelines*, AGD, Canberra, 2016, Appendix A, p. 24; H Clark and C Morris, 'Managing biometric information: the future is in the palm of your hands (and in your fingerprints, your iris and your facial features)', *Privacy Law Bulletin*, 14(6), August 2017, p. 94.
5. Clark and Morris, 'Managing biometric information: the future is in the palm of your hands (and in your fingerprints, your iris and your facial features)', op. cit.
6. Australian Law Reform Commission (ALRC), *For your information: Australian privacy law and practice*, report, 108, ALRC, Canberra, 2008, p. 407.
7. Explanatory Memorandum, Identity-matching Services Bill 2019, p. 3.
8. M Mann and M Smith, 'Automated facial recognition technology: recent developments and approaches to oversight', *University of New South Wales Law Journal*, 40(1), 2017, p. 122.

AFRT can be used to conduct 'one-to-one' matching (to verify an individual's identity) or 'one-to-many' searching (in which an image of a person can be compared with all images in a database in order to ascertain their identity).[9]

In other countries including the UK, US and Russia, AFRT has been integrated with CCTV systems to enable police to identify persons suspected of committing an offence or subject to an arrest warrant.[10] Similar technology has been trialled in some Australian jurisdictions, including the Northern Territory and Queensland.[11] For example, in 2015 the Northern Territory Government described its use of facial recognition technology as follows:

> Footage or images captured on CCTV footage can be submitted to NT Police's facial recognition team who can load it into the facial recognition system for analysis and comparison with existing images in the database.
>
> About 100,000 images have been copied into the system database from existing Police information holdings, with the first part of the trial in early 2015 successfully identifying around 300 individuals from photos and CCTV footage.[12]

Perth City Council is currently undertaking a twelve-month trial using facial recognition technology in cameras installed across East Perth. It has been reported:

> … success will be measured by how many times a lawful authority requested the use of the facial recognition capability and how many times a person of interest (which may include missing persons or lost children, as well as criminal suspects) is located. If successful, the council may consider expanding it.[13]

Biometric collection and face recognition is already used extensively in connection with immigration control and the issuing of visas. The *Migration Act 1958* authorises immigration officials to collect biometric data (referred to as 'personal identifiers') from citizens and non-citizens entering or leaving Australia.[14] This can include fingerprints and handprints, height and weight measurements, face images, audio or video recordings, an iris scan or signature.[15] Visa applicants located in certain countries are required to provide biometric information (usually their facial image and fingerprints) at the time they lodge their application.[16]

Facial recognition technology and biometric templates are currently used by airport smartgates to verify a traveller's identity by comparing their ePassport photo with a live image captured at the smartgate.[17] This is being further developed to allow for contactless processing, in which the face

---

9. Ibid., p. 123.
10. Ibid., pp. 123–4; S Levin, 'Half of US adults are recorded in police facial recognition databases, study says', *The Guardian*, 19 October 2016; V Dodd, 'Met police to use facial recognition software at Notting Hill carnival', *The Guardian*, 5 August 2017; C McGoogan, 'Facial recognition fitted to 5,000 CCTV cameras in Moscow', *The Telegraph (UK)*, 29 September 2017.
11. A Guest, 'Facial recognition software trials in Queensland alarm privacy advocates', *ABC News*, 10 March 2017; A Giles (Chief Minister of the Northern Territory) and P Chandler (Minister for Police, Fire and Emergency Services NT), *Facial recognition technology for police to help keep Territorians safe*, media release, 27 August 2015.
12. Giles and Chandler, *Facial recognition technology for police to help keep Territorians safe*, op. cit.
13. E Thomas, 'Perth council facial recognition trial greeted with concern and scepticism', *The Guardian (Australia)*, 12 June 2019; M Cormann (Minister for Finance and the Public Service) and A Tudge (Minister for Cities, Urban Infrastructure, and Population), *Perth Smart City project to improve citizen safety*, media release, 13 May 2019.
14. *Migration Act 1958* (Cth), section 257A. For further background about the development of the migration law with regards to biometrics, see: MA Neilsen, *Migration Amendment (Strengthening Biometrics Integrity) Bill 2015*, Bills digest, 111, 2014–15, Parliamentary Library, Canberra, 2015.
15. *Migration Act*, section 5A.
16. DOHA, 'Meeting our requirements—biometrics', DOHA website.
17. Australian Border Force (ABF), 'Entering and leaving Australia—SmartGates', ABF website.

matching can take place without a person needing to produce their passport.[18] A trial of such technology at Canberra Airport was paused in July 2019.[19] In March 2018, DOHA announced a $44.2 million contract with Unisys Australia for the provision of a new Enterprise Biometric Identification Services (EBIS) system. It is reported that the new system will match face images and fingerprints of people wishing to travel to Australia against biometric watch lists, in order to identify people of concern.[20]

The Australian Criminal Intelligence Commission (ACIC) also provides a number of biometric matching services to federal, state and territory police, including through the National Criminal Investigation DNA Database and National Automated Fingerprint Identification System (NAFIS).[21] However, its planned Biometric Identification Services Project ('BIS project'), which was intended to replace the NAFIS and develop a facial recognition capability for law enforcement agencies, was terminated in June 2018 following delays and a blowout in the projected costs.[22] In January 2019, the Auditor-General released a performance audit report on the ACIC's administration of the BIS project, which NEC Australia had been contracted to carry out. It found the ACIC had not effectively managed the project, and that none of the project's milestones or deliverables had been met despite a total expenditure of $34 million.[23]

In April 2019, the Parliamentary Joint Committee on Law Enforcement tabled the report on its inquiry into the impact of new and emerging information and communications technology.[24] It noted the termination of the BIS project, and endorsed a recommendation of the Law Council of Australia that the Australian Government take the following considerations into account when developing future strategies for biometric data and facial recognition systems:

- the development of an appropriate regime for detecting, auditing, reporting on, responding to and guarding against events that may breach biometric data security

- the use of methods for assessing the implications of any security breach and communicating the breach to both the general public and the technical, privacy and security communities and

- publicly releasing additional technical information about the nature of the facial matching scheme, and the process for ensuring that there are not false matches, in order to inform the public about its operation and to allow informed debate about its use and future database links.[25]

Identity crime in Australia

In his second reading speech for the IMS Bill, the Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs, David Coleman, stated that the identity-matching services provided for in the Bill will:

---

18. C Petrie, *Migration Amendment (Visa Revalidation and Other Measures) Bill 2016*, Bills digest, 51, 2016–17, Parliamentary Library, Canberra, 2016, pp. 5–6, 13–14; S Trask, 'Airport trial of SmartGate technology', *The Canberra Times*, 30 November 2017, p. 12; M O'Sullivan, 'Your face will be your passport', *The Sydney Morning Herald*, 22 February 2018, p. 1.
19. J Hendry, 'Australia's airport smartgate upgrade stalls', *iTnews*, 15 July 2019.
20. A Hawke (Assistant Minister for Home Affairs), *Enormous boost to Australia's biometric capability*, media release, 19 March 2018; J Hendry, 'Unisys to provide Australia's new biometrics travel platform', *iTnews*, 19 March 2018.
21. Australian Criminal Intelligence Commission (ACIC), 'Biometric matching', ACIC website, last updated 21 June 2019.
22. J Hendry, 'NEC loses national biometrics database project', *iTnews*, 15 June 2018; S Whyte, 'Biometrics deal dumped after delays, blowout', *The Canberra Times*, 16 June 2018, p. 3.
23. Australian National Audit Office (ANAO), *The Australian Criminal Intelligence Commission's administration of the Biometric Identification Services project*, Auditor-General Report, 24, 2018–19, 21 January 2019, p. 8.
24. Parliamentary Joint Committee on Law Enforcement, *Impact of new and emerging information and communications technology: report*, The Committee, Canberra, April 2019.
25. Ibid., p. 87 (recommendation 7).

> … help to protect Australians from identity crime, which continues to be one of the most common crimes in Australia. One in four Australians will be a victim of identity crime at some point in their lives, with an estimated annual direct cost of more than $2 billion to the economy. The face verification service will also help people to reclaim their lost or stolen identification documents faster, without the need re-establish their identity.[26]

As part of the Australian Government's National Identity Security Strategy (NISS), the Australian Institute of Criminology (AIC) and the Australian Bureau of Statistics (ABS) have produced a series of reports on identity crime in Australia, drawing on data from federal, state and territory agencies and surveys. The most recent reports estimate the cost of identity crime in Australia in 2015–16 to be $2.65 billion.[27] This figure includes direct and indirect losses incurred by government agencies and individuals, and the cost of identity crimes recorded by police. They estimated the costs of preventing and responding to identity crime during this period for Commonwealth, state and territory agencies (excluding state and territory police) to be $271 million, and $175.7 million for state and territory police.[28]

Surveys conducted by the AIC have found that over 20 per cent of respondents each year report having experienced misuse of personal information at some time in the past.[29] The AIC's 2017 survey found a significant increase in respondents experiencing misuse of their personal information in the previous 12 months (13.1 per cent, compared with 8.5 per cent in 2016) and in the proportion of respondents incurring out-of-pocket losses as a result of this misuse (9.6 per cent, up from 4.9 per cent in 2016).[30] Personal information and identity credentials are obtained from a variety of sources, including physical theft, accidental loss, automated telemarketing calls, and online phishing and malware attacks.[31]

Identity crime and national security

The Government has also drawn attention to the national security implications of identity crime. In his second reading speech, Minister Coleman highlighted the connections between identity crime and organised crime, stating:

> Identity crime is a key enabler of serious and organised crime, including terrorism.
>
> Australians previously convicted of terrorism related offences are known to have used fake identities to purchase items such as ammunition, chemicals that can be used to manufacture explosives, and mobile phones to communicate anonymously to evade detection.
>
> Identity crime is aided by the growing sophistication of criminal syndicates and the technology now able to support them in manufacturing fake identity documents.[32]

---

26. D Coleman, 'Second reading speech: Identity-matching Services Bill 2019', House of Representatives, *Debates*, (proof), 31 July 2019, p. 11.
27. P Jorna and RG Smith, *Identity crime and misuse in Australia 2017*, AIC Reports—Statistical Report 10, Australian Institute of Criminology, 30 December 2018, pp. x–xi; RG Smith and P Jorna, 'Counting the costs of identity crime and misuse in Australia, 2015–16', AIC, *Statistical Bulletin*, 15, 30 December 2018, p. 6 (this Bulletin provides a more detailed and precise costs breakdown). The reports use the term 'identity crime' broadly, as covering 'activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of crime'.
28. Smith and Jorna, 'Counting the costs of identity crime and misuse in Australia, 2015–16', op. cit., pp. 15–19.
29. Jorna and Smith, *Identity crime and misuse in Australia 2017*, op. cit., p. 35.
30. Jorna and Smith, *Identity crime and misuse in Australia 2017*, op. cit., p. xii.
31. Jorna and Smith, *Identity crime and misuse in Australia 2017*, op. cit., p. 7.
32. Coleman, 'Second reading speech: Identity-matching Services Bill 2019', op. cit.

National security concerns were also emphasised by COAG at the time of the signing of the *Intergovernmental Agreement on Identity Matching Services*, with a Communiqué stating that the agreement:

> … will help to protect Australians by making it easier for security and law enforcement agencies to identify people who are suspects or victims of terrorist or other criminal activity, and prevent the use of fake or stolen identities — which is a key enabler of terrorism and other serious crime.[33]

There appears to be little publicly available data regarding the connections between identity crime and organised crime. The ACIC, and previously the Australian Crime Commission (ACC), have identified identity crime as a key enabler of organised crime for some time, with the ACC's first *Organised Crime in Australia* report in 2007 reporting identity crime to be increasing and 'fundamental to many organised crime activities'.[34] Internationally, the European Union's law enforcement agency Europol has similarly reported document fraud to be a key facilitator for organised crime, with the production and use of fraudulent documents being linked to a range of crime areas including drug and people trafficking, migrant smuggling, money laundering and terrorism.[35]

The ACIC has identified identity crime as one of the key enablers of serious financial crime, and reports that personal identifying information is traded and sold by criminals to serious and organised crime groups.[36] At the same time, the ACIC suggests that identity crime is likely to become more prevalent with the increased online use and storage of personal information:

> As more financial services are provided online, there is a requirement for more personal identifiers, such as personal identification numbers, passwords, access codes and security questions, to be created and stored. These personal identifiers are of value to criminal entities and will continue to be harvested, sold and used in fraud and to access systems for other criminal purposes.
>
> Identity takeover is likely to emerge as the primary identity crime methodology used to facilitate financial crime, rather than identity creation. As government agencies and private institutions increase services offered online, it is likely that new identity crime enabled financial crime methodologies will be observed.[37]

This highlights the difficulties faced by governments in responding to the fraudulent use of identity information, as an increased reliance on personal identifiers to verify a person's identity also leads to large amounts of personal identification data being collected, shared and stored.

National Identity Security Strategy

In 2007, heads of COAG signed an *Intergovernmental Agreement on a National Identity Security Strategy* (NISS), aimed at combatting identity theft and the fraudulent use of stolen and assumed identities.[38] The parties agreed to strengthen government processes and standards for identifying

33. COAG, *Special meeting of the Council of Australian Governments on Counter-Terrorism: Communiqué*, COAG meeting, Canberra, 5 October 2017, p. 1.
34. Australian Crime Commission (ACC), *Organised crime in Australia*, ACC, Canberra, 2007, p. 9.
35. Europol, *European Union serious and organised crime threat assessment 2017*, Europol, Netherlands, 2017, pp. 20–1.
36. ACIC, *Serious financial crime in Australia 2017*, ACIC, Canberra, 2017, p. 15.
37. Ibid., p. 17.
38. COAG, *Intergovernmental Agreement to a National Identity Security Strategy*, April 2007, p. 2.

(and verifying the identity of) persons, including through enhancing the interoperability of biometric security measures.[39]

The NISS was revised in 2012.[40] The revised strategy highlights the importance of a shared approach to the protection of identity information, noting:

> Identity crime and misuse is a cross-border activity. It operates on a national and international scale – and will exploit weaknesses in one jurisdiction to obtain benefits in another. This is particularly relevant in Australia, where individuals build their identity with a combination of credentials. These credentials can be issued by multiple jurisdictions, and are often mutually recognised.
>
> Jurisdictions have a mutual reliance on the integrity of each other's identity security frameworks. If one jurisdiction has a less rigorous framework for allocating an identity credential, then it can be exploited.[41]

Reflecting this, one goal of the revised NISS 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.[42]

Document Verification Service

Another initiative arising out of the NISS was the Document Verification Service (DVS), which has been operational in the public sector since 2009.[43] The DVS 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 has not expired or been cancelled.[44] In a similar way to the identity-matching services provided for in the IMS Bill, data is not stored on the DVS itself; instead, requests to verify a person's identifying information are encrypted and sent through a secure 'DVS hub' to the issuing authority.[45] The person must provide express consent for their personal information to be used in this way.[46]

The private sector has had access to the DVS since May 2014.[47] Additionally, in November 2015 Australia reached an agreement with New Zealand to allow government agencies and businesses to verify identity documents issued by either country.[48] Businesses seeking to use the DVS must meet criteria set out in the access policy—this includes being subject to Australia's privacy laws (or the New Zealand equivalent), having a physical presence in Australia or New Zealand, and the use or disclosure of the information being either required by an Australian law or reasonably necessary for the organisation's activities or functions.[49]

---

39. Ibid., clauses 6 and 7.
40. AGD, *National Identity Security Strategy 2012*, AGD, Canberra, 2013.
41. Ibid., p. 9.
42. AGD, *National Identity Security Strategy: a National Biometric Interoperability Framework for government in Australia*, [AGD], [Canberra], 2014, p. 2.
43. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit., clause 4.1.
44. DOHA, 'Document verification service', DOHA website, last updated 22 January 2019.
45. Ibid.; Document Verification Service (DVS), 'How the DVS works', DVS website, last updated 15 May 2018.
46. DVS, 'The DVS and consent', DVS website, last updated 16 January 2018.
47. G Brandis (Attorney-General), *Helping business combat identity crime and streamline online services*, media release, 5 May 2014.
48. M Keenan (Minister for Justice) and P Dunne (New Zealand Minister of Internal Affairs), *Australia–New Zealand agreement to help combat identity crime*, media release, 11 November 2015.
49. DOHA, *Document verification service (DVS) commercial service: access policy*, DOHA, Canberra, version 4, n.d., p. 2.

There has been a rise in both private and public sector usage of the DVS since 2014. The 2017 AIC report on *Identity Crime and Misuse in Australia* found that 513 private-sector organisations and 79 government entities used the service at 30 June 2017, compared with 350 private-sector organisations and 45 government agencies the previous year.[50] The DVS can be used to verify information relating to most government-issued identity credentials, including four documents identified by the report as being at particular risk of misuse: Medicare cards, driver licences, birth certificates and passports.[51]

The Explanatory Memorandum to the IMS Bill identifies shortcomings in the capacity of the DVS to detect all forms of identity crime:

> [the DVS] 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 used by the document-issuing agency. These documents are not detected by the DVS because the biographical details are genuine.[52]

National Facial Biometric Matching Capability

The development of systems to support the sharing and matching of facial images across jurisdictions has been in progress for some years. In October 2014, a meeting of COAG's then Law, Crime and Community Safety Council (LCCSC)[53] noted the Commonwealth's plans to establish a National Facial Biometric Matching Capability (Capability), which would provide a mechanism for the cross-jurisdictional sharing of existing information collected by agencies.[54] In subsequent meetings the LCCSC affirmed its support for the Capability and took steps towards the development of an intergovernmental agreement on state and territory participation.[55]

In September 2015, the Minister for Justice, Michael Keenan announced that the Commonwealth was spending $18.5 million to develop the Capability, as part of a broader series of measures to combat terrorism and identity crime.[56] The announcement—which corresponded with the release of the *Identity Crime and Misuse in Australia 2013–14* report—noted that the Capability would initially involve 'one-to-one' image-based verification between 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.[57] Minister Keenan stated:

---

50. Jorna and Smith, *Identity crime and misuse in Australia 2017*, op. cit., pp. xvi, 52–3.
51. Ibid., pp. 52–3.
52. Explanatory Memorandum, IMS Bill, p. 46.
53. 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. See: AGD, 'Law, Crime and Community Safety Council', AGD website.
54. LCCSC, *Communique*, COAG Meeting, Canberra, 3 October 2014, p. 2.
55. For example: LCCSC, *Communique*, COAG Meeting, Canberra, 22 May 2015, p. 2; LCCSC, *Draft communique*, COAG Meeting, Canberra, 5 November 2015, p. 2; LCCSC, *Communique*, COAG Meeting, Canberra, 19 May 2017, p. 7.
56. M Keenan (Minister for Justice), *New $18.5 million biometrics tool to put a face to crime*, media release, 9 September 2015.
57. Ibid.

> The report by the Attorney-General's Department and the AIC estimates that identity crime costs Australia around $2 billion per year, and supports findings from the Australian Crime Commission that identity crime is one of the key enablers of terrorism and organised crime.
>
> … 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.[58]

The Face Verification Service (FVS) commenced operation in November 2016, enabling the Department of Foreign Affairs and Trade (DFAT) and the Australian Federal Police (AFP) 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.[59]

Intergovernmental agreement

On 5 October 2017, at a special meeting of COAG on counter-terrorism, all state and territory leaders signed the *Intergovernmental Agreement on Identity Matching Services* (IGA), providing for the sharing and matching of identity information across jurisdictions.[60] The objective of the IGA is to:

> … facilitate the secure, automated and accountable exchange of identity information, with robust privacy safeguards, in order to prevent identity crime and promote law enforcement, national security, road safety, community safety and service delivery outcomes.[61]

The IGA provides for the exchange of identity information through six specified Identity Matching Services, and other services subsequently developed under the auspices of the Agreement. Of the six named services, at least two—the DVS and FVS—are already in operation. The National Identity Security Coordination Group (Coordination Group) is responsible for developing and maintaining the policies and procedures governing access to each of the services. Participating agencies will also enter into a common Participation Agreement which provides the framework within which the agencies negotiate the details of data sharing arrangements.[62]

Schedules to the IGA set out the financial contributions from each state and territory as well as the particular agencies that will have access. The ACT's participation is subject to limitations: as well as providing that its participation must be consistent with the *Human Rights Act 2004* (ACT), Schedule G of the IGA states that the Territory will only allow access to its data for certain purposes, and will not participate in the 'One Person One Licence System'.[63]

Information about how the identity-matching scheme will operate is set out in the *Key Issues and Provisions* section below.

---

58. Ibid.
59. M Keenan (Minister for Justice), *New face verification service to tackle identity crime*, media release, 16 November 2016.
60. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit.
61. Ibid., p. 4 (clause 1.1).
62. Ibid., clauses 7.2–7.6.
63. Ibid., Schedule G, A.11, p. 45; T McIlroy, 'Barr a lone voice for civil liberties', *The Canberra Times*, 6 October 2017, p. 4.

State and territory legislation

The IGA does not provide agencies with the legal authority to share information through these services—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.

Queensland was the first jurisdiction to pass new legislation on this front, with the *Police and Other Legislation (Identity and Biometric Capability) Amendment Act 2018* (Qld) enacted in March 2018.[64] This amended a range of transport and policing laws to authorise Queensland's participation in the identity matching scheme. Following the passage of the Bill, the Queensland Minister for Police and Corrective Services, Mark Ryan stated that the Bill:

> … will be of real benefit to those tasked with the security of the Commonwealth Games, which represents a once-in-a-lifetime event that will demonstrate to the world the great things Queensland has to offer.
>
> We are expecting both international and interstate guests to attend so I encourage the Federal Government and all states and territories to ensure this legislation is passed in time for the Commonwealth Games.[65]

However, an evaluation conducted by the Queensland Police Service after the 2018 Gold Coast Commonwealth Games reportedly found problems with the rollout of the system, including the following:

> Difficulties were experienced in data ingestion into one of the systems with the testing and availability not available until the week Operation Sentinel [the Games security operation] commenced…
>
> The inability of not having the legislation passed, both Commonwealth and state, in time for the Commonwealth Games reduced the database from an anticipated 46 million images to approximately eight million.[66]

The ABC reported that while police records had been included in the system, images from Queensland's Department of Transport and other sources had not been used. It also reported that none of the 16 'high-priority targets' requested as part of the operation could be identified, and that halfway through the Games, the system was opened up to 'basic policing'.[67]

In November 2018, NSW Parliament passed the *Road Transport Amendment (National Facial Biometric Matching Capability) Act 2018*, which amended the *Road Transport Act 2013* (NSW) to authorise certain government agencies to share information through the identity-matching scheme.[68] A Parliamentary inquiry into the Bill before it was passed noted that the NSW Government had indicated:

> … at the present stage Roads and Maritime Services has no plans to access or use the Capability, only to provide information to the hub. However, the witnesses noted that in the future the agency may

64. *Police and Other Legislation (Identity and Biometric Capability) Amendment Act 2018* (Qld).
65. M Ryan (Queensland Minister for Police, Minister for Corrective Services), *Queensland leads nation to strengthen security measures*, media release, 7 March 2018.
66. J Bavas, 'Facial recognition system rollout was too rushed, Queensland police report reveals', *ABC News online*, 6 May 2019.
67. Ibid.
68. Parliament of NSW, 'Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018'.

> consider signing up to the One Person One Licence Service…another identity-matching service envisaged under the Intergovernmental Agreement which will be available to assist States in upholding the integrity of driver licence and other identification systems.[69]

While no other jurisdiction to date has passed legislation in relation to the scheme, the Minister's second reading speech notes that five states now have the legislative frameworks in place to implement the IGA.[70] Tasmania has amended its driver licensing Regulations to authorise the disclosure of protected information for the purposes of identity-matching services.[71] Existing laws in South Australia[72] and Victoria[73] are also considered to facilitate implementation of the IGA.[74]

Privacy and data security

Biometric data and privacy concerns

The increasing use of biometric systems and templates has amplified concerns regarding the privacy and data security implications of this technology. In a speech to the Biometrics Institute in 2010, the then Deputy Privacy Commissioner, Timothy Pilgrim stated that the collection and handling of biometric information attracts strong public concern because:

> … biometric information is about a person's physical characteristics. When we collect biometric information from a person, we are not just collecting information **about** that person, but information **of** that person.
>
> Biometric information cuts across both information privacy and physical privacy. It can reveal sensitive information about us, including information about our health, genetic background and age, and most importantly, it is **intrinsic** to each of us.[75]

In 2008, the ALRC identified a number of general privacy concerns arising from the use of biometric technologies, including:

- widespread use of biometric systems enables extensive monitoring of the activities of individuals, particularly where the same form of biometric information is used to identify individuals in a number of different contexts
- biometric technologies, such as facial recognition technologies, may be used to identify individuals without their knowledge or consent
- biometric information could be used to reveal sensitive personal information, such as information about a person's health or religious beliefs
- the security of biometric systems could be compromised and

---

69. NSW Legislative Council Standing Committee on Law and Justice, *Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018*, Report, 65, 12 November 2018, pp. 4–5.
70. Coleman, 'Second reading speech: Identity-matching Services Bill 2019', op. cit., p. 12.
71. Vehicle and Traffic (Driver Licensing and Vehicle Registration) Amendment (Identity Matching Services) Regulations 2017 (Tas).
72. *Public Sector (Data Sharing) Act 2016* (SA), section 13 permits the Minister to enter into data-sharing agreements.
73. *Road Safety Act 1998* (Vic), sub-paragraph 90K(a)(vi) permits the use or disclosure of information collected or received by the Roads Corporation in relation to its registration or licensing functions and activities, for the purposes of giving effect to an intergovernmental agreement.
74. DOHA, Submission to the NSW Legislative Council Standing Committee on Law and Justice, *Inquiry into the Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018*, 31 October 2018, p. 3.
75. T Pilgrim (Deputy Privacy Commissioner), *Privacy in Australia: challenges and opportunities*, speech to Biometrics Institute, Sydney, 27 May 2010.

- the accuracy and reliability of many biometric systems remains unknown, creating the potential for serious consequences for an individual who is falsely accepted or rejected by such a system.[76]

As noted by the ALRC, particular concerns arise with the collection of facial data, as unlike the collection of fingerprints or DNA, facial images can be captured from a distance and without the knowledge or consent of the individual.[77] Furthermore, faces are difficult to hide or alter, and therefore the misuse of this information can be more prolonged than credit card or tax file number data, which can be replaced.[78]

Public discussion and reporting on the Capability has situated it within the broader context of governmental data collection, data-matching and data security. Questions have been raised about the security of data stored and shared as part of the Capability, particularly in light of incidents which have drawn attention to potential vulnerabilities in government and non-government systems.[79] This includes reports in 2017 that the Medicare details of any Australian were being sold to order through a darknet auction site, and a mass data breach at US credit agency Equifax which exposed the personal data of 143 million US customers.[80]

Bruce Arnold, a law academic and director of the Australian Privacy Foundation, has argued that Australia's privacy laws are insufficient to protect against misuse or inadvertent disclosure of biometric information:

> The sharing occurs in a nation where Commonwealth, state and territory privacy law is inconsistent. That law is weakly enforced, in part because watchdogs such as the Office of the Australian Information Commissioner (OAIC) are under-resourced, threatened with closure or have clashed with senior politicians.
>
> Australia does not have a coherent enforceable right to privacy. Instead we have a threadbare patchwork of law (including an absence of a discrete privacy statute in several jurisdictions).[81]

Privacy Act and biometric data

The proposed identity-matching services will be subject to existing privacy laws. The *Privacy Act 1988* (Cth), and the Australian Privacy Principles (APPs) made under this Act regulate the handling of personal information by Commonwealth government agencies as well as private sector organisations with an annual turnover of more than $3 million, all private health service providers and some other small businesses.[82] Most states and territories also have privacy laws regulating their respective public sector agencies.[83]

---

76. ALRC, *For your information: Australian privacy law and practice*, op. cit., pp. 408–9.
77. Ibid.; Mann and Smith, 'Automated facial recognition technology: recent developments and approaches to oversight', op. cit., p. 123.
78. Mann and Smith, 'Automated facial recognition technology: recent developments and approaches to oversight', op. cit., p. 131; A Molnar, 'Your face is part of Australia's "national security weapon": should you be concerned?', *The Conversation*, 14 September 2015.
79. R Trigger, 'Experts sound alarm as biometric data from drivers' licences added to government database', *ABC News*, 16 January 2018; E Thomas, 'Coalition could allow firms to buy access to facial recognition data', *The Guardian (Australia)*, 26 November 2017.
80. P Farrell, 'The Medicare machine: patient details of "any Australian" for sale on darknet', *The Guardian (Australia)*, 4 July 2017; A Andriotis and R McMillan, 'Equifax slammed for huge data hack', *The Australian*, 11 September 2017.
81. B Arnold, 'Let's face it, we'll be no safer with a national facial recognition database', *The Conversation*, 6 October 2017.
82. *Privacy Act 1988* (Cth); OAIC, 'Privacy Act', OAIC website, last updated 29 July 2019; OAIC, 'Privacy for organisations—small business', OAIC website, last updated 15 August 2019.
83. OAIC, 'Privacy in your state', OAIC website, last updated 6 August 2019.

Under the *Privacy Act*, biometric information used for the purpose of automated biometric verification or identification, as well as biometric templates, is classified as 'sensitive information'.[84] Sensitive information is generally afforded a higher level of protection than other personal information, in recognition of the adverse consequences which may flow from the inappropriate handling of such information.[85] Limitations include that sensitive information can only be collected with consent (unless a specified exception applies) and can only be used or disclosed for a secondary purpose to which it was collected if this is directly related to the primary purpose of collection.[86] However, it is an exception to these restrictions if the collection, use or disclosure is required or authorised by an Australian law.

Notifiable data breaches scheme

The Notifiable Data Breaches scheme came into effect on 22 February 2018, and applies to agencies and organisations with obligations under the APPs. It requires entities to notify the Australian Information Commissioner and affected individuals about data breaches which are likely to cause serious harm. The notification must include recommendations about the steps individuals should take in response to the breach.[87]

Privacy impact assessments

In August 2015, a privacy impact assessment (PIA) was carried out in relation to the design and initial operation of the interoperability hub system, through which agencies can request and share facial image data, during its early stages of development.[88] The PIA, conducted by Information Integrity Solutions Pty Ltd (IIS), found that the hub design process and proposed governance arrangements were generally consistent with the requirements of the APPs. At the same time, it highlighted the broad scope of the Capability and the privacy risks associated with the proposed system as a whole:

> … it is important to recognise that the Hub will have an impact on the circumstances in which facial biometric information is shared, by whom and the volume of images shared, and these risks will have to be actively managed. There is also the risk, which IIS considers is low, that the Hub and the metadata generated by transactions performed through it could potentially allow for some tracking or surveillance of individuals' everyday activities. However, it is the view of IIS that the privacy impacts of the whole system could well be greater than the risks at individual agency or Hub level. As such, IIS considers that strong, widely respected governance of the system as a whole as, particularly as it evolves over time, is equally and potentially more important than governance of the individual participating agencies and the Hub.[89]

In recognition of these risks, the PIA made a series of recommendations to strengthen privacy practices in the design and operation of the hub. This included limiting the metadata generated by the hub, strictly controlling access to one-to-many matching and clarifying the limits on the initial scope of the Capability, as well as including an independent representative on relevant governance bodies to provide the 'people's voice'.[90] The AGD accepted or partially accepted all

---

84. *Privacy Act*, section 6.
85. OAIC, 'Chapter B: key concepts', *APP guidelines*, OAIC website, version 1.3, 22 July 2019.
86. *Privacy Act*, Schedule 1, APP 3 and APP 6.
87. OAIC, 'Notifiable data breaches', OAIC website.
88. Information Integrity Solutions, *National Facial Biometric Matching Capability privacy impact assessment—interoperability hub*, report carried out for Attorney-General's Department, August 2015.
89. Ibid., p. 5.
90. Ibid., pp. 5–7. For analysis of the PIA and the Government's response, see: B Arnold, 'A national identity hub? The privacy impact assessment for the National Facial Biometric Matching Scheme', *Privacy Law Bulletin*, 13(3), March 2016, pp. 50–3.

recommendations, though did not support the suggestion of a people's representative, stating that the public interest would be represented through the OAIC's involvement in the Coordination Group, and consultation with state and territory privacy commissioners and/or ombudsmen.[91]

In 2016, AGD commissioned an independent PIA on the initial use of the Face Verification Service by federal government departments to access citizenship and visa data held by the (then) Department of Immigration and Border Protection. It reported that the PIA found the exchange of data via the FVS to be 'privacy positive', due to the service controlling the disclosure of data and maintaining clear audit trails. The PIA made five recommendations to address privacy risks and concerns that may be heightened with increasing use of the FVS.[92] A copy of the PIA has not been publicly released.

A Memorandum of Understanding is currently in place between the OAIC and the Attorney-General's Department for the OAIC to conduct privacy assessments of:

- the AGD's management of the interoperability hub and
- the governance, operation and information security of the National Driver Licence Facial Recognition Solution, provided for in the IMS Bill.[93]

The first report was due to be completed by 1 October 2018, but does not appear to have been publicly released. The second is due by 1 October 2019.[94]

Committee consideration

Parliamentary Joint Committee on Intelligence and Security

A review by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into the 2018 Bills lapsed at the dissolution of the House of Representatives on 11 April 2019.[95] The inquiry had received 20 submissions and had held two public hearings at the time it lapsed.

The PJCIS is currently undertaking a review of the reintroduced Bills, and has accepted as evidence all submissions and transcripts from the previous review.[96] Further details can be found at the inquiry homepage.

Senate Standing Committee for the Scrutiny of Bills

The Senate Standing Committee for the Scrutiny of Bills has not yet reported on the current Bills, but issued a report on the 2018 Bills on 14 February 2018.[97] A key area of concern identified by the Committee was the privacy implications of the IMS Bill, and the fact that a number of safeguards identified in the explanatory materials (and in the IGA) are not included in the Bill itself.[98] The Committee noted that the IMS Bill's provisions would:

---

91. AGD, *Preliminary privacy impact assessment of the National Facial Biometric Matching Capability–interoperability hub: Attorney-General's Department response*, December 2015.
92. AGD, 'Summary of the privacy impact assessment for the Face Verification Service', AGD, November 2016.
93. OAIC, 'MOU with AGD—National Facial Biometric Matching Capability', OAIC website, last updated 21 May 2019.
94. Ibid., Schedule 2.
95. Parliamentary Joint Committee on Intelligence and Security (PJCIS), 'Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018', Parliament of Australia website.
96. PJCIS, 'Review of Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019', Inquiry homepage.
97. Senate Standing Committee for the Scrutiny of Bills, *Scrutiny digest*, 2, 2018, The Senate, 14 February 2018, pp. 14–15 (Passports Bill), 20–8 (IMS Bill).
98. Ibid., pp. 20–4.

> … give a broad power for the Home Affairs department to collect, use and disclose personal information for a wide range of purposes to a wide range of government agencies (and some local government authorities and private entities) … The Bill has clear implications for the privacy of the millions of individuals whose facial images and other biographical information will be available for collection, use and disclosure.[99]

Although acknowledging that the explanatory materials provided a detailed analysis of the Bill's privacy implications, and set out a number of safeguards to help protect privacy, the Committee raised concerns that the Bill may 'unduly trespass on personal rights and liberties' due to the breadth of the authorised disclosures. It noted that potential safeguards such as access criteria, requirements for privacy impact assessments and limitations on the amount of information released by the systems, are contained in the IGA but not in the Bill. The Committee sought the Minister's advice as to whether the intended policy and administrative safeguards could be included as legal requirements in the Bill, or alternatively whether the Bill could include a requirement that such safeguards be implemented by agencies seeking access to identity-matching services.[100]

The Minister for Home Affairs responded to the Committee's comments on 4 April 2018, and the Committee considered this response in its report on 9 May 2018.[101] On the issue of privacy safeguards, the Minister stated that the protections contained in the Bill, and obligations imposed by the IGA, already provide a 'strong degree of protection for the information transmitted through the identity-matching services'.[102] He further noted that the identity-matching services will be 'supported by a broad system of controls and arrangements that govern the provision and use of the services', with the IMS Bill being just one aspect of this.[103] In response, the Committee reiterated its concerns about the adequacy of safeguards in the IMS Bill.[104]

Concerns raised by the Committee in relation to specific provisions are discussed in the *Key Issues and Provisions* section below.

Policy position of non-government parties/independents

The Australian Labor Party does not appear to have commented on the Bills directly. The IGA was agreed to by all state and territory leaders, including Labor leaders in Queensland, Victoria, Northern Territory, ACT, Western Australia and South Australia. However, the ACT and Victorian Governments have both stated that the IMS Bill goes beyond the scope of the IGA.[105]

At the time the IGA was reached, then Opposition Leader Bill Shorten offered cautious support for the identity-matching system, stating:

> We think that biometric technology can be a real addition in terms of keeping Australians safe. But of course, when it comes to the final detail, we'll wait to see what the final detail from the Government is.

---

99. Ibid., p. 22.
100. Ibid., pp. 23–4.
101. Senate Standing Committee for the Scrutiny of Bills, *Scrutiny digest*, 5, 2018, The Senate, 9 May 2018, pp. 103–120.
102. Ibid., p. 109.
103. Ibid., p. 108.
104. Ibid., p. 110.
105. Victorian Government, Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018*, n.d., p. 3; F O'Mallon, 'ACT raises clash with facial recognition law', *The Canberra Times*, 13 May 2018, p. 9.

> But I just want to reassure Australians that Labor takes a bipartisan approach to good ideas about keeping Australians safe.[106]

Shadow Attorney-General, Mark Dreyfus has also stated:

> … on the face of it, these measures appear sensible; but we will wait to see the detail of what is being proposed … It is important that the balance between security and privacy is maintained in the face of new threats and there are appropriate protections in place.[107]

The Australian Greens have expressed opposition to the measures, with justice spokesperson Senator Nick McKim stating: 'creating a massive database of people's photographs is a privacy invasion that creates a honeypot for hackers'.[108]

Other minor parties and independents have not commented on the measures to date.

Position of major interest groups

Civil liberties and privacy organisations have expressed strong concern about the privacy implications of the identity-matching scheme in general. In October 2017, immediately following the signing of the IGA, organisations including the Australian Privacy Foundation, Digital Rights Watch and state and territory civil liberties groups issued a joint statement condemning the creation of a national facial database. The statement described the database as 'an unnecessary and disproportionate invasion of the privacy rights of all Australians' and 'fundamentally incompatible with a free and open society'.[109]

These concerns were reiterated in submissions to the PJCIS inquiry in 2018. A number of submissions argued that the IMS Bill is not a proportionate response to the harms it is purporting to address, and may enable substantial infringements on the privacy rights of individuals.[110] A joint submission by Future Wise and the Australian Privacy Foundation contended that the broad purposes of the Bill—which include removing duplicate records and targeting avoidance of traffic fines as well as detecting terrorism—undermine a case for the proportionality of the Bill's measures:

> There appears to be no need, for example, to expose all Australian citizens to biometric data matching to remove duplicate records. It is incumbent on government to design other methods of record management that do not involve significant privacy incursions.

106. B Shorten (Leader of the Opposition) and J Ryan, *Joint doorstop interview: Australian manufacturing; COAG; Turnbull's gas crisis; Australian wool*, transcript, Melbourne, 4 October 2017.
107. K Murphy, 'Turnbull denies new facial recognition measures amount to "mass surveillance"', *The Guardian (Australia)*, 5 October 2017.
108. Ibid.
109. Digital Rights Watch, *Comprehensive national face database incompatible with a free society*, media release, 6 October 2017.
110. Future Wise and Australian Privacy Foundation, Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018*, March 2018, p. 7; Australian Lawyers for Human Rights (ALHR), Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018*, 20 March 2018, p. 3; Law Council of Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018*, 21 March 2018, p. 3.

> … The extent of the law enforcement activities contemplated by the Bill should therefore be re-examined, to be limited to those absolutely necessary for public safety—rather than those that are simply convenient or 'efficient'.[111]

Interest groups have expressed doubts about the adequacy of the governance frameworks for the identity-matching services, and the safeguards contained in the IMS Bill.[112] One particular concern has been that many of the rules for access to the services will be contained in access policies and participation agreements made under the intergovernmental agreement. These are not referenced in the Bill. The Office of the Victorian Information Commissioner expressed concern that managing compliance through such instruments 'may not be sufficiently robust', noting that they may not be enforceable and could allow 'fundamental controls to be amended without parliamentary oversight'.[113] This point was similarly made by the Queensland Office of the Information Commissioner, which submitted that the IMS Bill 'does not adequately embed into law the core intents of the regime to which the Governments have agreed'.[114]

In addition to questions about the adequacy of safeguards built into the scheme, some stakeholders also suggested that Australia's privacy laws do not provide sufficient protection against possible misuse of information under the scheme.[115] A number of submissions raised the possibility of establishing an independent authority responsible for oversight of the retention, collection and use of biometric information, citing the UK's creation of a Commissioner for the Retention and Use of Biometric Material.[116]

It was also suggested that further information about the identity-matching scheme may be required to enable proper consideration of the IMS Bill. For example, the Law Council of Australia argued that insufficient information is available regarding the technical aspects of scheme:

> It is difficult … to comment further on the nature and operation of the Interoperability Hub or various identity matching services as there has been very little information released by the Government on their technical development.
>
> …The Law Council is 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.[117]

Other organisations, including Civil Liberties Australia and the Queensland Office of the Information Commissioner, raised concerns that Privacy Impact Assessments have not yet been

---

111. Future Wise and Australian Privacy Foundation, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 7.
112. Future Wise and Australian Privacy Foundation, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 11–12; Office of the Victorian Information Commissioner (OVIC), Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018*, 21 March 2018; Queensland Office of the Information Commissioner (QOIC), Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018*, March 2018, pp. 4–5.
113. OVIC, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 1, 3.
114. Ibid., p. 3.
115. ALHR, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 3–4; Future Wise and Australian Privacy Foundation, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 11–12.
116. Law Council of Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 8; Joint councils for civil liberties, Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018*, 21 March 2018, pp. 4–5; Future Wise and Australian Privacy Foundation, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 11–12.
117. Law Council of Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 4.

completed and published in relation to all services referred to in the Bill and the various uses to be made of them.[118]

Support for the measures has been largely based on a security rationale. Anthony Bergin, a senior analyst at the Australian Strategic Policy Institute (ASPI), expressed support for the scheme as provided for in the IGA, arguing that 'most Australians would be surprised to learn that police don't have this capability and would be disturbed by the heightened risks faced by our law enforcement officers'.[119]

Stakeholder comments in relation to specific provisions of the two Bills are discussed under the *Key issues and Provisions* section below.

Financial implications

The Explanatory Memorandum to the IMS Bill states that it does not propose any new expenditure and the overall financial impact is low.[120]

As indicated in the background, the Capability received funding of $18.5 million over four years in the 2014–15 Mid-Year Economic and Fiscal Outlook. Further funding of $2.5 million was provided in the 2017–18 Budget to complete the Capability's build.[121]

The IGA specifies that the Commonwealth is responsible for the establishment costs for this system and for 50 per cent of annual operating and maintenance costs. It will also be responsible for the ongoing costs of maintaining and operating the DVS hub and interoperability hub.[122] Each state and territory has committed to a specific financial contribution towards the ongoing operating and maintenance costs of the National Driver Licence Facial Recognition Solution.[123]

Statement of Compatibility with Human Rights

As required under Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth), the Government has assessed the Bills' compatibility with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of that Act. The Government considers that the Bills are compatible.[124]

Parliamentary Joint Committee on Human Rights

The Parliamentary Joint Committee on Human Rights has not yet reported on the Bills, but reported on the 2018 Bills on 27 March 2018.[125] The Committee queried whether the measures are a proportionate limitation on the right to privacy, and sought advice from the Minister for

---

118. Civil Liberties Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018*, 21 March 2018, p. 3; QOIC, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 3.
119. A Bergin, 'Information-sharing among agencies key to national security', Australian Strategic Policy Institute (ASPI) website, 13 October 2017.
120. Explanatory Memorandum, IMS Bill, p. 5.
121. Explanatory Statement, Financial Framework (Supplementary Powers) Amendment (Attorney-General's Portfolio Measures No. 2) Regulations 2017; Senate Legislation and Constitutional Affairs Legislation Committee, *Official committee Hansard*, 26 February 2018, p. 118.
122. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit., Part 10.
123. Ibid., Schedules A to H.
124. The Statements of Compatibility with Human Rights can be found at pages 40–58 of the Explanatory Memorandum to the IMS Bill and pages 4–7 of the Explanatory Memorandum to the Passports Bill.
125. Parliamentary Joint Committee on Human Rights, *Human rights scrutiny report*, 3, 2018, 27 March 2018, pp. 41–51.

Home Affairs (in relation to the IMS Bill) and Minister for Foreign Affairs (in relation to the Passports Bill) on this point.

The Committee raised particular concerns about the scope of the IMS Bill and queried whether the provisions governing access to facial images and other biometric data are sufficiently circumscribed for each of the identity matching services.[126] It noted:

> As the Hub will permit access to driver licences, the personal information of a significant proportion of the adult Australian population will be retained. A centralised facility for searching such large repositories of facial images and biometric data is a very extensive limitation on the right to privacy… There is a serious question as to whether having databases of, and facilitating access to, facial images of a very significant portion of the population in case they are needed is the least rights restrictive approach to achieving the stated objectives of the measure.[127]

The Committee also raised questions about the types of information which may be used—such as social media photographs and historical facial images—and the extent to which the hub will effectively protect against misuse of such information, particularly in relation to vulnerable groups.[128] It noted that international human rights case law has raised concerns about the compatibility of biometric data retention programs with the right to privacy, where the programs involve an indiscriminate or open-ended retention of data.[129] It further queried whether the *Privacy Act* provides an adequate safeguard for the purposes of international human rights law.[130]

Key issues and provisions

The IMS Bill is intentionally limited in scope—it is not designed to give effect to the spectrum of information-sharing arrangements and procedures envisioned under the IGA. Instead, it should be seen as one piece of a patchwork of laws and policies which will regulate the use of identity-matching services.

The Bill establishes an express legal basis for the Department of Home Affairs (DOHA) to provide identity-matching services and places restrictions on the circumstances in which the services may be used and types of information involved. It does not authorise particular agencies to use the services. Organisations seeking access must be authorised to collect, use and disclose identification information by some other federal, state or territory law. They will also need to meet criteria as specified in the IMS Bill, IGA and in various access policies and agreements made under the IGA.

How does the system work?

Identity-matching facilities

The IMS Bill expressly authorises DOHA to develop, operate and maintain two facilities through which identity-matching services are provided. The system is intended to operate based on a 'hub and spoke' model, in which the Commonwealth operates the centralised facilities through which state and territory agencies (and other participating entities) communicate with each other to

126. Ibid., pp. 43–6, 49.
127. Ibid., p. 46.
128. Ibid., pp. 46–9.
129. Ibid., p. 47.
130. Ibid., pp. 45–6.

request or provide information.[131] Details about how these facilities will operate is largely contained in the IGA, rather than in the provisions of the Bill.

Clause 14 of the Bill provides that DOHA may develop, operate and maintain the ***interoperability hub***, through which agencies and organisations may electronically relay requests for the provision of identity-matching services, and transmit information in response to such requests.[132] Agencies will access the hub (at least initially) via a web-based user interface into which they log in to manually enter search requests. The IGA provides that over time, the hub will also be able to receive requests via 'system-to system connections with Agencies' existing systems'.[133] Identification information of an individual is not stored in the hub itself—in his second reading speech for the 2018 IMS Bill, Minister for Home Affairs, Peter Dutton explained:

> The hub is not a database and does not conduct any facial biometric matching. Rather it acts like a router, transmitting matching requests received from user agencies to facial image databases. These databases conduct the matching using facial recognition software and return a response back via the hub.[134]

The second facility provided for in the Bill is the National Driver Licence Facial Recognition Solution (NDLFRS).[135] This is a federated database of the identity information contained in government identification documents, such as (but not necessarily limited to) driver licences.[136] Each state and territory road agency will have its own partitioned data store, with individual agency-based access controls. Unlike the interoperability hub, the NDLFRS will store identification information contributed by state and territory agencies. It will be connected to the interoperability hub to facilitate data sharing with other agencies.[137]

The IGA provides that the Commonwealth, though it hosts and operates the database, will not have the ability to view or modify the information within each partitioned data store.[138] However, the Bill itself does not place any express restrictions on DOHA's ability to access, collect or disclose information held in the system.[139] Furthermore, the NDLFRS will also include common facial biometric matching software and 'a central store of biometric templates, derived from facial images replicated by the states and territories using the facial biometric matching software'. Both the software and templates will be managed by the Commonwealth Data Hosting Agency (CDHA).[140]

---

131. Explanatory Memorandum, IMS Bill, p. 28.
132. IMS Bill, **clause 14**.
133. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit., clauses 6.10–6.11.
134. P Dutton, 'Second reading speech: Identity-matching Services Bill 2018', House of Representatives, *Debates*, 7 February 2018, p. 485.
135. IMS Bill, **clause 15**.
136. The IGA provides that other types of facial images may be included in the ***NDLFRS*** at the request of a state or territory—it provides the examples of images on firearms licences and proof of age cards (clause 6.18).
137. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit., clause 6.16.
138. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit., subclause 6.16(c).
139. For example, see the authorisation provisions at **clauses 17 to 18**, discussed under 'What are the limitations on access?' below.
140. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit., clause 6.15.

Identity-matching services

The Bill provides that the interoperability hub is to be used for the purposes of requesting and providing 'identity-matching services'.[141] **Subclause 7(1)** states that an ***identity-matching service*** is any of the following:

- a **face identification service** (***FIS***), defined under **subclause 8(1)** as a service which involves electronically comparing the facial image of a person with the identification information of one or more persons contained in government identification documents (often referred to as 'one to many' matching)[142]
- a **face verification service** (***FVS***), defined under **subclause 10(1)** as a service comparing the identification information about a person with information contained in a particular government identification document, where a facial image of the person is included in the request and/or in a response to the request (also known as 'one to one' matching).[143] Unlike ***FIS***, the service is aimed at verifying—rather than ascertaining—a person's identity
- a **facial recognition analysis utility service** (***FRAUS***), defined under **clause 9** as the electronic comparison of a person's facial image with identification information about the person supplied by the same state or territory authority, which is included in a database in the NDLFRS. The comparison must be for the purpose of assessing the accuracy or quality of information held by the relevant authority[144]
- the **One Person One Licence service** (***OPOLS***), in which a person's facial image and other identification information is compared with information included in a NDLFRS database, for the purpose of determining whether the person holds multiple government identification documents[145] and
- an **identity data sharing service** (***IDSS***), defined under **clause 11** as a service, other than the four services listed above, which involves a disclosure of a person's identification information through the interoperability hub. The disclosure must be between Commonwealth, state or territory authorities and for the purpose of an ***identity or community protection activity*** (explained below).[146]

Minister's power to prescribe additional services

Additionally, **paragraph 7(1)(f)** gives the Minister the power to make rules prescribing other services as ***identity-matching services***, where they:

- involve the collection, use and disclosure of identification information and
- involve the interoperability hub or NDLFRS.[147]

Any such rules are in the form of a disallowable legislative instrument.[148] The Minister may prescribe services which permit access by local government authorities or non-government entities if the purpose of the service is for identity verification and certain other conditions are met (these are discussed under 'private sector access').[149] The Bill requires the Minister to consult

141. IMS Bill, **clause 14**.
142. IMS Bill, **paragraph 8(1)(a)**.
143. IMS Bill, **subclause 10(1)**.
144. IMS Bill, **clause 9**.
145. IMS Bill, **clause 12**.
146. IMS Bill, **clause 11**.
147. IMS Bill, **paragraph 7(1)(f)**.
148. IMS Bill, **clause 30**.
149. IMS Bill, **subclause 7(2)**.

with the Human Rights Commissioner and Information Commissioner about the proposed rules, though does not provide further guidance as to the nature of any consultation.[150]

The Queensland Office of the Information Commissioner has raised concerns that the breadth of the rule-making power under **paragraph 7(1)(f)** may allow the Minister to prescribe 'many-to-many' matching services or blanket surveillance. It has recommended that the provision expressly exclude such services.[151]

What information may be shared?

Identification information

The IMS Bill provides for the collection, use and disclosure of ***identification information***. The scope of this term is set out under **clause 5**, which provides that it may be information about a living, dead, real or fictitious person and encompasses:

- current and former names and addresses, place and date of birth, and age (including an age range)
- the current or former sex, gender identity or intersex status of the person
- information about whether the person is alive or dead
- any information contained in or associated with a person's driver licence, or other licence or identity document issued by a state or territory authority
- the person's current or former citizenship, any information about a visa the person holds or has held, and any information contained in or associated with an Australian or foreign travel document and
- a facial image of the person, biometric template derived from the image or the result of a biometric comparison involving such an image.[152]

The Minister may also make rules (in the form of a disallowable legislative instrument) prescribing other types of information to be identification information.[153] Before doing so, the Minister must be satisfied that the information that can be used to identify an individual (whether alone or in conjunction with other information), is reasonably necessary for the provision of an identity-matching service and assists one or more identity or community protection activities. The Minister must also consult with the Human Rights Commissioner and Information Commissioner.[154]

Additionally, the IMS Bill specifies information which is not ***identification information*** and which therefore cannot be collected, used or disclosed under the Bill. This includes information or an opinion about a person's:

- racial or ethnic origin
- political opinions, philosophical beliefs or religious beliefs or affiliations
- membership of a political association, professional or trade association or trade union
- sexual orientation or practices
- criminal record or

150. IMS Bill, **subclause 7(5)**.
151. QOIC, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 3, 5.
152. IMS Bill, **subclause 5(1)**.
153. IMS Bill, **paragraph 5(1)(n) and clause 30**.
154. IMS Bill, **subclause 5(4)**.

- health or genetics.[155]

However, where information is not **primarily** one of the above kinds, but nonetheless allows such information about a person to be reasonably inferred (for example, where a person's racial or ethnic origin may be inferred through their name or place of birth), this may still be ***identification information*** and subject to disclosure.[156]

What are the limitations on access?

As indicated in Minister Coleman's second reading speech, the IMS Bill does not in itself authorise government agencies or other entities to use identity-matching services, though it provides a broad framework under which the services can operate.[157] An agency or organisation must have a separate legal basis on which it is authorised to disclose information for the purpose of participating in identity-matching services.

As indicated above, in addition to legislative authorisation to disclose information, an agency's ability to access these services will be based on a combination of requirements set out in either or both the Bill and IGA. In particular, the IGA (but not the Bill) provides that participating bodies must meet the criteria set out in the relevant Access Policy, developed by the Coordination Group.

155. IMS Bill, **subclause 5(2)**.
156. IMS Bill, **subclause 5(3)**.
157. D Coleman, 'Second reading speech: Identity-matching Services Bill 2019', op. cit., p. 13.

Face Verification Service—access policy

The Access Policy for the Face Verification Service 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 FVS
- undertake or contribute to a **privacy impact assessment (PIA)** to account for every information flow which occurs through the FVS, to which the agency is a party (unless the agency's use of the FVS is exempt from the relevant Commonwealth, state or territory privacy laws)
- enter into an **Interagency Data Sharing Arrangement (IDSA)** with each agency with which it intends to share information via the FVS. The Access Policy states that where possible, classes of agencies with like functions should enter into common, multilateral agreements
- maintain a register of **Nominated Users** who are authorised to submit queries via the FVS, 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 FVS at least once every financial year and
- enter into a **memorandum of understanding** with DOHA in relation to the services through the interoperability hub.[158]

The content of the IDSA must include details of the IDSA's agreed duration, arrangements for dispute settlement, non-compliance and termination, as well as arrangements for assigning costs associated with the FVS (where relevant). The IDSA must identify the scope of the data-sharing arrangements (such as the accreditation requirements and access permissions for users, maximum number of Nominated Users and method of access, and agreed maximum number of transactions) and the arrangements for protecting personal information shared via the FVS.[159]

DOHA is responsible for reviewing IDSAs to ensure consistency with the Access Policy, and for reviewing audit and compliance reports.

Authorisations

Although the IMS Bill does not authorise particular agencies to participate in the identity-matching services, **Part 3** of the Bill does provide authorisation for DOHA to collect, use and disclose identification information in connection with these services and articulates the scope of the Department's powers in this area.

Clause 17 authorises DOHA to collect identification information where the collection is via an electronic communication to the interoperability hub or the NDLFRS, and for one of the purposes set out in **subclause 17(2)**. The purposes for which collection is authorised include:

158. AGD, 'Face Verification Service (FVS)—access policy', AGD, Canberra, June 2017, pp. 2–5. This policy has not yet been updated in light of the machinery of government changes in December 2017; however, DOHA, rather than AGD, is now responsible for managing agencies' access to identity-matching services, including through entering into MOUs and reviewing ISDAs: DOHA, 'Face matching services', DOHA website, last updated 22 January 2019.
159. Ibid.

- providing or developing an identity-matching service for the purpose of an ***identity or community protection activity*** (explained below)
- developing, operating or maintaining the NDLFRS or
- protecting a person who has acquired an assumed identity under the *Crimes Act 1914* (Cth) or is involved in a Commonwealth, state or territory witness protection program.[160]

Clause 18 enables DOHA to use or disclose identification information collected through an electronic communication to the interoperability hub or NDLFRS, or held in or generated using the NDLFRS. Again, the use or disclosure must be for one of the purposes set out in **subclause 17(2)**.

Clause 19 specifies that where a state or territory law limits the disclosure of identification information by a state or territory authority (or by a body or person acting on behalf of the authority), but provides an exemption for disclosures authorised by a Commonwealth law, then such an authority, body or person will be permitted to disclose identification information to DOHA for inclusion in the NDLFRS. The Explanatory Memorandum states this is intended to facilitate the disclosure of driver licence data by states and territories, where the existing legislation allows disclosures authorised by Commonwealth law:

> This is to reduce the number of states and territories that would need to amend their own legislation before Home Affairs could develop the database.[161]

Identity or community protection activity

As explained above, DOHA will be authorised to collect, use and disclose identification information in developing or providing an identity-matching service for the purpose of an ***identity or community protection activity***. Additionally, certain identity-matching services provided for in the Bill—in particular the ***FIS*** and ***IDSS***—can only be accessed in the course of such an activity.

Clause 6 provides a definition of ***identity or community protection activity***, as an activity covered by one of the following categories:

- preventing and detecting identity-related fraud, including the use of stolen or fraudulently obtained government identification documents (or identification information from such documents)[162]
- law enforcement—that is, the preventing, detecting, investigating or prosecuting an offence against a Commonwealth, state or territory law or in relation to proceedings (or potential proceedings) under the *Proceeds of Crime Act 2002*[163]
- national security—conducting an investigation or gathering intelligence relevant to Australia's national security[164]
- protective security—promoting the security of an asset, facility or person associated with government, including by checking the background of a person with access to such an asset/facility or by protecting a person under witness protection/with a legally assumed identity[165]

160. IMS Bill, **subclause 17(2)**.
161. Explanatory Memorandum, IMS Bill, p. 31.
162. IMS Bill, **subclause 6(2)**.
163. IMS Bill, **subclause 6(3)**.
164. IMS Bill, **subclause 6(4)**.
165. IMS Bill, **subclause 6(5)**.

- community safety—promoting community safety, including by identifying an individual who has suffered or is reasonably believed to be at risk of suffering physical harm or an individual who is reasonably believed to be involved with a significant risk to public health or safety[166]
- road safety activities, including promoting the integrity of driver licensing systems[167] and
- verifying the identity of an individual.[168]

The Scrutiny of Bills Committee noted the breadth of some of these purposes, arguing that the sharing of information in relation to any federal, state or territory offence, for road safety or for identity information more broadly:

> … could allow state and territory agencies to share and seek to match facial images and other biographical information for persons suspected of involvement in very minor offences, such as jaywalking, or for verifying the identity of an individual for any purpose.[169]

Submissions to the PJCIS inquiry also raised concerns about the breadth of these categories. The joint submission by Future Wise and the Australian Privacy Foundation suggested that terms such as community safety or road safety:

> … are defined so widely as to potentially draw almost all activities within the Bill's ambit. The effect is that biometric matching might be deployed for almost any purpose without limit.[170]

Australian Lawyers for Human Rights noted that many of the purposes under **clause 6** 'relate not to uncovering of wrongdoing that has already occurred, but 'prevention' and 'promotion' activities', and objected to the use of identity-matching services where there is no clear connection to a likely offence.[171]

Face identification service (FIS)

The ***FIS***, in providing for one-to-many matches, is one of the more controversial measures in the IGA, as it can involve the use and disclosure of images (and other personal information) of multiple persons who may have no connection to the person in the original image. Reflecting this, the IMS Bill and IGA place greater restrictions on use of this service than on the other services which form part of the scheme.

One restriction, noted above, is that the ***FIS*** can only be used for the purpose of identifying the individual in the original image, or determining whether they have multiple identities, in the course of an ***identity or community protection activity*** covered by any of **subclauses 6(2) to 6(6)**.[172] This will capture most categories of the definition of ***identity and community protection activity*** set out above, but will not allow access for the purposes of road safety activities or identity verification.

This largely reflects the IGA's list of permitted purposes for which agencies may use the FIS.[173] One notable difference is in relation to the 'law enforcement activities' category—the IGA states that

166. IMS Bill, **subclause 6(6)**.
167. IMS Bill, **subclause 6(7)**.
168. IMS Bill, **subclause 6(8)**.
169. Senate Standing Committee for the Scrutiny of Bills, *Scrutiny digest*, 2, 2018, op. cit., p. 23.
170. Future Wise and Australian Privacy Foundation, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 5.
171. Australian Lawyers for Human Rights, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 5.
172. IMS Bill, **paragraph 8(1)(b)**.
173. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit., clause 4.21.

where the sharing is between agencies in different jurisdictions, the service may only be used for activities relating to an offence which carries a maximum penalty of at least three years imprisonment.[174] This limitation is not replicated in the Bill. The Explanatory Memorandum notes this but does not explain the reason for the omission, stating:

> The Bill will not specifically restrict this activity to offences that carry a maximum penalty of not less than three years imprisonment … but it is intended that this restriction will apply on a policy basis. Any amendment to the provisions of the IGA … will be by agreement between the Commonwealth and the states and territories. As with all of the identity or community protection activities, state or territory agreement will be required before a jurisdiction's data can be used in relation to additional offences.[175]

The absence of any lower limit in the Bill in regards to offences appears to envision future changes to the IGA that expand the offences for which the ***FIS*** may be used. Possibly in connection with this, the IGA provides that twelve months after the ***FIS*** commences operation, the Coordination Group will review the definition and operation of the general law enforcement purpose, and 'should consider whether the definition maximises the utility of the FIS for law enforcement agencies, while maintaining appropriate privacy safeguards'.[176] Without amendments to the IGA, it is unlikely—but theoretically possible—that agencies could use the ***FIS*** to ascertain the identity of a person suspected of committing a minor infringement.

A second restriction is in relation to who may access the ***FIS***. **Subclause 8(2)** provides a list of authorised agencies—this includes the Australian Border Force;[177] Australian Crime Commission; Australian Federal Police; ASIO; a federal Department administered by a Minister administering citizenship, migration or passports legislation; and state and territory police forces and anti-corruption agencies. The Minister may prescribe further authorities in the rules, but only where satisfied that the authority has a function previously performed by one of the specified state or territory agencies.[178]

Private sector access

Another concern that has been raised in relation to the IGA and IMS Bill is the extent to which they allow the private sector to access personal information contained in government databases. The use of identity-matching services by private sector entities and local government authorities will be regulated by a combination of provisions under the IMS Bill, the IGA and access policies developed under the agreement.

Restrictions under the Bill

The IMS Bill provides that, of the five services expressly provided for under the IGA, non-government entities and local government authorities can potentially access the face verification service (***FVS***) only. Such organisations will be able to request information about an individual through the ***FVS*** if:

- verifying the individual's identity is reasonably necessary for one or more of the organisation's functions or activities

---

174. Ibid., subclause 4.21(b), clause 4.22.
175. Explanatory Memorandum, IMS Bill, p. 16.
176. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit., clause 4.25.
177. The ABF may request the service only so far as it is investigating or prosecuting an offence against the *Customs Act 1901*, *Crimes Act 1914*, *Criminal Code* or *Environment Protection and Biodiversity Conservation Act 1999*: IMS Bill, **paragraph 8(2)(a)**.
178. IMS Bill, **paragraph 8(2)(q) and subclause 8(3)**.

- the individual has consented to the organisation using and disclosing their identification information for the purpose of verifying their identity
- the organisation carries on activities in Australia from premises located in Australia, or resides in Australia and
- either the *Privacy Act* applies to the organisation, or in the case of a local government authority, it is bound by a state or territory law or has entered into a written agreement with DOHA which provides for the protection of personal information (and means of recourse for affected individuals) comparable to that provided by the Australian Privacy Principles.[179]

Restrictions under the IGA

Additionally, the IGA states that private sector access to the ***FVS*** to match information held by the states and territories is subject to:

- the express approval of the relevant minister 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
- compliance with a 'FVS Commercial Service Access Policy' developed by the Coordination Group (including a fee for service arrangement) and
- an FVS Commercial Service audit and compliance program, overseen by the Coordination Group.[180]

The Law Council of Australia has argued that these restrictions provided for in the IGA are 'important safeguards that should be incorporated into the Bill'.[181] Furthermore, it notes that the Bill does not provide for penalties for private organisations where they make an unauthorised use of the hub or identification information, and suggests the existing controls are insufficient.[182]

On the issue of consent, the Law Council has suggested that further information is needed as to how informed consent will be recorded and verified to a standard that enables access to the FVS.[183] Other interest groups have questioned the adequacy of this consent requirement. The joint submission to the PJCIS inquiry by the Australian councils for civil liberties, which opposed private sector access to the identity-matching services, argued:

> In all cases, consent should be valid, free and voluntary. This is quite often not the case when no real choice or alternative is offered and there is little or no opportunity to opt out.[184]

The Office of the Victorian Information Commissioner has also raised concerns about private sector and local government access to the scheme, stating:

> The variation in the quality of governance and security that can be expected, particularly from local government, raises issues in relation to the adequacy of information management practices and personal information protection. The potential for scope creep—in that personal information may be

179. IMS Bill, **subclauses 7(3) and (4)**.
180. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit., clause 5.4.
181. Law Council of Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 6.
182. Ibid., p. 6.
183. Ibid., p. 5.
184. Joint councils for civil liberties, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 5–6.

> used for additional purposes other than those for which it was initially collected—is also a significant concern.[185]

What protections are in place?

Disclosure offence

The IMS Bill creates an offence of recording or disclosing ***protected information*** when the person making the record or disclosure has obtained the information in their capacity as an ***entrusted person***.[186] The maximum sentence for the offence is imprisonment for two years. It is an exception to the offence where the conduct is either authorised by, or in compliance with, a Commonwealth, state or territory law.[187]

An ***entrusted person*** is defined broadly as:

- the Secretary or an APS employee in DOHA
- an officer or employee of a Commonwealth agency or authority, state, territory or foreign government or authority, or public international organisation, whose services are made available to DOHA or
- a contractor engaged to provide services to DOHA in connection with the interoperability hub or NDLFRS (or officer or employee of such a contractor).[188]

Protected information is:

- identification information obtained from the NDLFRS or from an electronic communication to or from the NDLFRS or interoperability hub
- information about the making, content or addressing of such an electronic communication, or about identification information held in the NDLFRS or
- information that enables access to the hub or NDLFRS.[189]

The Scrutiny of Bills Committee raised concerns with the provision, in which authorised disclosure of information is an exception to the offence, rather than the offence being drafted to apply only to 'unauthorised' disclosures. The Committee has pointed out that the *Criminal Code Act 1995* provides that a defendant who wishes to rely on an exception bears an evidential burden.[190] This means that a defendant who believes the disclosure or recording was authorised must raise evidence on this point (though does not need to positively prove the matter). The Committee has noted that the explanatory materials do not address the issue and asked the Minister to advise why an 'offence-specific defence' is being used in this instance. It has suggested:

> … it may be appropriate if proposed subclause 21(1) was amended to provide that a person commits the offence if the conduct is not authorised by, or in compliance with a requirement under, a law of the Commonwealth or of a State or Territory.[191]

In response, the Minister stated that if this defence was included as an element of the offence itself, 'it would be extremely difficult for the prosecution to establish that the conduct was not

185. OVIC, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 2.
186. IMS Bill, **subclause 21(1)**.
187. IMS Bill, **subclause 21(2)**.
188. IMS Bill, **subclause 21(4)**.
189. IMS Bill, **subclause 21(4)**.
190. Senate Standing Committee for the Scrutiny of Bills, *Scrutiny digest*, 2, 2018, op. cit., pp. 26–7.
191. Ibid., p. 27.

authorised under any law', whereas an entrusted person should be aware of the legislative basis on which they are relying when disclosing information.[192] The Minister suggested the Bill ensures that in handling protected information, the onus is on an entrusted person to show a level of care commensurate with the sensitivity of the information.[193] The Committee requested that this information be included in the Explanatory Memorandum, and reiterated its concerns about the appropriateness of reversing the evidential burden of proof in this case.[194] The Explanatory Memorandum for the 2019 Bill does not provide further information on this point.

When will disclosure be authorised?

Clauses 22 to 25 set out circumstances in which the recording and disclosure of protected information will be authorised, and therefore act as exceptions to the disclosure offence under **clause 21**. An entrusted person may disclose or record protected information:

- for the purposes of the *Identity-matching Services Act 2018* or in the course of exercising powers or performing functions or duties in relation to the interoperability hub or NDLFRS[195]
- if the person reasonably believes the disclosure is necessary to lessen or prevent a serious and imminent threat to the life or health of an individual, and makes the disclosure for this purpose[196]
- where the disclosure is to the Integrity Commissioner in relation to a corruption issue (within the meaning of the *Law Enforcement Integrity Commissioner Act 2006*)[197] or
- where the information relates to the affairs of a person and the person has consented to the recording or disclosure (and the recording or disclosure is in accordance with that consent).[198]

Minister's rule-making power and the obligation to consult

Clause 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
- necessary and convenient to carry out or give effect to the Act.

There are some specified limitations on the rules—they cannot create an offence or civil penalty; provide powers of arrest or detention, entry, search or seizure; impose a tax or create an appropriation; or directly amend the text of the Act.[199] The rules are subject to disallowance as well as sunsetting.[200]

As explained above, in exercising his power to make rules prescribing additional types of identification information or additional identity-matching services, the Minister will be required to consult the Information Commissioner and Human Rights Commissioner.[201]

---

192. Senate Standing Committee for the Scrutiny of Bills, *Scrutiny digest*, 5, 2018, op. cit., p. 116.
193. Ibid.
194. Ibid., p. 117.
195. IMS Bill, **clause 22**.
196. IMS Bill, **clause 23**.
197. IMS Bill, **clause 24**.
198. IMS Bill, **clause 25**.
199. IMS Bill, **subclause 30(2)**.
200. IMS Bill, **subclauses 30(3) and (4)**.
201. IMS Bill, **subclauses 5(4) and 7(5)**.

The Scrutiny of Bills Committee welcomed the Bill's inclusion of this requirement to consult. However, the Committee suggested that the requirement be strengthened by making such consultation a condition of the validity of the legislative instrument. [202] The Committee also queried the inclusion of significant matters such as this in a rule rather than in Regulations, noting that Regulations are subject to a higher level of executive scrutiny as they must be drafted by the Office of Parliamentary Counsel and approved by the Federal Executive Council.[203]

The Law Council raised similar concerns, suggesting that there are risks that through these provisions, the scope of the identity-matching scheme could be determined by delegated rather than primary legislation. It has also queried whether either the Australian Human Rights Commission or Office of the Australian Information Commissioner are sufficiently resourced to take on this additional consultation role.[204] The Law Council recommended that the consultation requirement be amended to include a requirement for the Minister to report to the public on the results of these consultations, and any reasons for departing from advice provided by the commissioners, before making a relevant rule.[205]

In response to the concerns raised by the Scrutiny of Bills Committee, the Minister accepted the Committee's recommendation that the Minister be required to have regard to any submissions made by the commissioners prior to making the rules, and if the rules depart from the commissioners' advice, provide reasons for this. He indicated he would propose Government amendments to this effect.[206] However, no changes have been made to the 2019 IMS Bill to incorporate such a requirement. On the question of the appropriateness of rules rather than Regulations, the Minister pointed to the Office of Parliamentary Counsel's *Drafting Direction No. 3.8 – Subordinate Legislation*, which provides that its starting point is that subordinate instruments should be made in the form of legislative instruments (as distinct from Regulations), and noted that the Bill expressly prohibits certain matters from being prescribed in rules.[207] The Committee stated it would make no further comment on the matter.[208]

Annual reporting requirement

Clause 28 requires the Secretary of DOHA to give a report to the Minister at the end of each financial year, for tabling in each House of Parliament, with statistics relating to all requests from Commonwealth, state and territory authorities (except ASIO) for an FIS, FVS or OPOLS. The statistics are to be broken down by requesting authority, service requested, number of requests in which information (or confirmation of identity) was provided and those in which no information or confirmation was provided, and in the case of the FIS, the kind of ***identity or community protection activity*** for which the service was requested.[209]

The Secretary must similarly report statistics on requests made by non-government entities for an FVS. However, this data is not required to identify the particular organisations, but rather the total

202. Senate Standing Committee for the Scrutiny of Bills, *Scrutiny digest*, 2, 2018, op. cit., p. 25.
203. Ibid.
204. Law Council, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 4–5.
205. Ibid.
206. Senate Standing Committee for the Scrutiny of Bills, *Scrutiny digest*, 5, 2018, op. cit., pp. 111–2. See Office of Parliamentary Counsel (OPC), *Drafting direction no. 3.8 – subordinate legislation*, OPC, July 2017.
207. Ibid., p. 112.
208. Ibid., p. 113.
209. IMS Bill, **paragraph 28(1)(a)**.

number of requests and total number of entities (as well as the number in which information was or was not provided).[210]

Additionally, for each government authority (other than ASIO) which used an IDSS to disclose or collect identification information, the Secretary must provide the name of the authority, a brief description of the nature of the information and an indication whether the authority collected or disclosed that information.[211] The report must also include any other information required by the Minister in relation to an identity-matching service or administration of the Act.[212]

Subclause 28(2) provides that the report must not 'unreasonably' disclose personal information about an individual. The Explanatory Memorandum notes that this is aimed at ensuring the report does not disclose personal information 'that is not reasonably required for accountability purposes'.[213] It states that this is not intended to prevent the inclusion of publicly available information about an individual.[214]

A number of stakeholders and interest groups have suggested that this reporting requirement be further strengthened. The Office of the Victorian Information Commissioner has noted that **clause 28** does not expressly require reporting on data breaches or misuse of the services:

> … it tells the public about the quantum of requests but little about the security of the data or the compliance of participants in the IMS ecosystem.[215]

Noting that the new Notifiable Data Breaches scheme will not capture all agencies and bodies accessing the identity matching services (such as state and territory government organisations), the Office suggested that another mechanism be inserted into the Bill to include specific reporting relating to instances of unauthorised or inappropriate access and the remedial action taken in response.[216] It suggests that the complex nature of the identity-matching scheme makes this particularly important:

> …The inter-related nature of the Bill, the IGA and the other agreements also makes assurance of compliance activities more complex, and is another reason for more transparent reporting.[217]

The Law Council has criticised the fact that the reporting requirements do not capture non-government entities or ASIO. Although noting that the Explanatory Memorandum states this is due to considerations of commercial confidentiality, it has argued that 'the public have a right to know which non-government entities have access to the Face Verification Service'.[218] It has further suggested that restrictions on the reporting of ASIO-related data 'should be determined on a case by case basis and not included … as a blanket exception'.[219] The Queensland Office of the Information Commissioner has similarly recommended that the reporting requirement be expanded to capture data breaches and incidents as well as non-government access to the FVS.[220]

---

210. IMS Bill, **paragraph 28(1)(b)**.
211. IMS Bill, **paragraph 28(1)(c)**.
212. IMS Bill, **paragraph 28(1)(d)**.
213. Explanatory Memorandum, IMS Bill, p. 38.
214. Ibid.
215. OVIC, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 2.
216. Ibid.
217. Ibid., p. 3.
218. Law Council of Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 7.
219. Ibid.
220. QOIC, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 4–5.

The Scrutiny of Bills Committee queried whether the reporting requirement should be extended to capture instances where information is disclosed pursuant to **clause 23** (disclosures to lessen or prevent a threat to life or health) or **clause 24** (disclosures relating to a corruption issue).[221] In response, the Minister accepted the suggestion in relation to **clause 23**, and indicated that he would propose an amendment to the Bill to accommodate this.[222] However, no such change has been included in the 2019 IMS Bill. In relation to reporting on information disclosed pursuant to **clause 24**, the Minister noted that such a requirement could jeopardise the confidentiality of disclosures, which may occur without the Secretary's knowledge, and that the Integrity Commissioner already has reporting requirements in relation to these types of disclosures under the *Law Enforcement Integrity Commissioner Act 2006*.[223] The Committee requested this information be included in the Explanatory Memorandum, and stated it would not comment further on the matter.[224] The Explanatory Memorandum for the 2019 IMS Bill does not include further information on this point.

Statutory review

The IMS Bill requires the Minister to cause a review of the operation of the Act and the provision of identity-matching services to be started within five years of the Act's commencement.[225] The report is to be tabled in each House of Parliament within 15 sitting days after it is received by the Minister.

This is a longer timeframe than specified in the IGA, which provides that a general review into the operation of the identity-matching services will be conducted three years from the commencement of the agreement. The IGA states that the review is to assess matters including the effectiveness of the services in progressing the objectives of the agreement, the effectiveness of governance arrangements, the privacy impacts and effectiveness of privacy safeguards in protecting personal information.[226] The terms of reference are to be set by the Coordination Group and the review is to be published online by the Commonwealth.

It is unclear whether the review provided for in the Bill is intended to be separate to that in the IGA, and the explanatory materials do not directly discuss this point. The Explanatory Memorandum states that a five year timeframe is necessary as:

> … it may take some time for all of the states and territories to commence participation in the identity-matching services, and sufficient operating time is needed to ensure that the functioning of the services in relation to all jurisdictions can be assessed adequately.[227]

The Queensland Office of the Information Commissioner has stated it would be preferable for the review to commence two years after commencement of the legislation, noting that this was recommended by the Queensland Parliamentary Legal Affairs and Community Safety Committee following its consideration of the Queensland Bill.[228] It has also suggested that it may be appropriate for the IMS Bill to specify 'critical components' of the review, such as 'expansion of

---

221. Senate Standing Committee for the Scrutiny of Bills, *Scrutiny digest*, 2, 2018, op. cit., pp. 27–8.
222. Senate Standing Committee for the Scrutiny of Bills, *Scrutiny digest*, 5, 2018, op. cit., p. 118.
223. Ibid., pp. 118–9.
224. Ibid., pp. 119-20.
225. IMS Bill, **clause 29**.
226. COAG, *Intergovernmental Agreement on Identity Matching Services*, op. cit., clause 13.3.
227. Explanatory Memorandum, IMS Bill, p. 38.
228. QOIC, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., p. 4.

services within the IMS regime, abuse of the system, mistakes arising from false positives ,[and] unintended outcomes of the IMS'.[229]

Passports Bill

Identity-matching capability

The Passports Bill amends the *Passports Act* to allow for the disclosure of personal information in relation to identity-matching services. Currently, section 46 of that Act provides that the Minister for Foreign Affairs may disclose personal information for a number of specified purposes—this includes law enforcement, confirming or verifying information about a passport applicant or facilitating a person's international travel.[230] Disclosure is limited to the types of information and persons specified by the Minister under the Australian Passports Determination 2015, and this is dependent on the particular purpose of disclosure.[231] There are currently three classes of information which may be disclosed (though not in all circumstances):

- ***data page information***, which means information contained on the data page of an Australian travel document, such as the document number, expiry date, and the name, data of birth, photograph and signature of the document holder
- ***status information***, which means information about whether the document is currently valid, including whether it has been lost or stolen or has restrictions on its use and
- ***authenticity information***, which is information necessary to establish the authenticity of a person applying for or holding an Australian travel document.[232]

Item 1 of the Passports Bill inserts **proposed paragraph 46(da)** into the *Passports Act* to provide that the Minister may disclose personal information for the purposes of participating in a service to share or match information relating to a person's identity. The service must be specified or of a kind specified in the Minister's determination.

The amendment does not appear to significantly expand the Minister's power to disclose personal information—section 46 already permits the disclosure of photographs to a wide range of federal, state and territory government agencies as well as Interpol and foreign border authorities. **Proposed paragraph 46(da)**, in providing a broad authority for disclosures expressly in relation to identity-matching services, will cover any existing gaps which might limit DFAT's capacity to participate in identity-matching services.

Computerised decision-making

Item 3 of the Passports Bill inserts **proposed section 56A** into the *Passports Act* to provide for computerised decision-making. This empowers the Minister to arrange for the use of computer programs to make decisions or exercise other powers of the Minister under the Act (or associated legislative instruments). The Minister is taken to have made the decision or exercised the relevant power that was made or exercised by the computer program.[233] **Proposed subsection 56A(3)** enables the Minister to substitute a decision for a decision made by a computer program, where satisfied that the decision made by the computer program is incorrect.

---

229. Ibid.
230. *Australian Passports Act 2005*, section 46.
231. Australian Passports Determination 2015 (Cth), clause 23.
232. Ibid., subclause 23(3).
233. Passports Bill, **proposed subsections 56A(1) and (2)**.

The Explanatory Memorandum provides that it is intended that automation will be used for 'low-risk decisions that a computer can make within objective parameters'.[234] In particular, it indicates that the provision will allow the Minister to arrange automated disclosures of personal information for the purposes of the identity-matching services, as provided for under **proposed paragraph 46(da)**, stating 'this is necessary to facilitate DFAT's full participation in the services, given that they will operate on an automated basis'.[235]

Proposed section 56A is in similar terms to computerised decision-making provisions in a broad range of other Acts.[236] The use of computer programs to automate government decision-making has been occurring in various forms for some time, with benefits including the ability for such programs to instantaneously apply complex rules and policies and reduce inaccuracy, inconsistency and bias in decision-making. However, there are also risks associated with automated decision-making, with the potential for seemingly minor programming errors to lead to large numbers of incorrect decisions.[237]

Submissions to the PJCIS inquiry raised concerns with this provision. Australian Lawyers for Human Rights argued that **proposed section 56A** is overly broad and does not distinguish between programs being used to assist in decision-making and to actually make the decision.[238] The Australian councils for civil liberties suggested that if the provision is to be enacted, the decisions which are made by computers and the data used to generate the decisions are made publicly available, and that 'strong procedural fairness criteria' be included.[239]

234. Explanatory Memorandum, Australian Passports Amendment (Identity-matching Services) Bill 2019, p. 3.
235. Ibid., p. 9.
236. For example: *Migration Act 1958*, section 495A; *Customs Act 1901*, section 126H; *Social Security (Administration) Act 1999*, section 6A; *A New Tax System (Family Assistance) (Administration) Act 1999*, section 223.
237. For further discussion of issues associated with automated decision-making, see: S Power and A Grove, *National Health Amendment (Pharmaceutical Benefits) Bill 2016*, Bills digest, 66, 2016–17, Parliamentary Library, Canberra, 22 February 2017, pp. 2–3, 6–7; C Petrie, *Veterans' Affairs Legislation Amendment (Digital Readiness and Other Measures) Bill 2016*, Bills digest, 68, 2016–17, Parliamentary Library, Canberra, 27 February 2017, pp. 3–5, 10.
238. ALHR, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 9–11.
239. Joint councils for civil liberties, Submission to Parliamentary Joint Committee on Intelligence and Security, op. cit., pp. 14–15.

Members, Senators and Parliamentary staff can obtain further information from the Parliamentary Library on (02) 6277 2500.