2016-2017-2018

THE PARLIAMENT OF THE
COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

AUSTRALIAN PASSPORTS AMENDMENT (IDENTITY-MATCHING SERVICES) BILL 2018

EXPLANATORY MEMORANDUM

(Circulated by authority of the Minister for Foreign Affairs,
the Hon Julie Bishop MP)

AUSTRALIAN PASSPORTS AMENDMENT (IDENTITY-MATCHING SERVICES) BILL 2018

OUTLINE

1. This Bill amends the *Australian Passports Act 2005* (Passports Act) to provide a legal basis for ensuring that the Minister is able to make Australian travel document data available for all the purposes of, and by the automated means intrinsic to, the identity-matching services to which the Commonwealth and the States and Territories agreed in the *Intergovernmental Agreement on Identity Matching Services* (IGA), signed at a meeting of the Council of Australian Governments on 5 October 2017.

2. The services will enable identity matching based on personal information held in government systems nationally. They include a number of biometric services in which the Department of Foreign Affairs and Trade intends to participate. One, the Face Verification Service (FVS), will allow Commonwealth, state and territory agencies, and potentially in future the private sector, to verify the known or claimed identities of individuals by reference to facial images in government identity records. Another, the Face Identification Service (FIS), will allow authorised facial recognition specialists in law enforcement, national security and anti-corruption agencies to identify unknown persons. Beyond the FVS and the FIS, an Identity Data Sharing Service will allow for the secure sharing of biometric identity information in other circumstances.

3. Subsidiary to the IGA, a Participation Agreement (PA) will regulate access to the services by individual Commonwealth, state and territory agencies. Among other things, the IGA provides that strict privacy, transparency and accountability controls must apply to all the services. The Department of Home Affairs will administer the services and oversee compliance with these controls.

4. The IGA identifies the purposes of the services as: preventing identity crime; general law enforcement; national security; protective security; community safety; road safety; and identity verification. Within this framework, data-holding agencies retain discretion to determine specific purposes for which, entities to which, and other circumstances under which, they make their data available through the services.

5. The services operate on an automated query and response basis. When data-holding agencies receive requests for information that satisfy parameters specified in bilateral data-sharing arrangements subsidiary to the PA, the requests will be processed and responses provided in a timeframe that precludes the exercise of human discretion in deciding whether to disclose the information in each case. The scale of expected future FVS use by large client-service agencies is a further factor that will make human intervention infeasible. It will also allow law enforcement and national security agencies to act without delay to identify people in circumstances where their liberty and physical security, or the liberty and physical security of others, are under threat, and take time-critical action to prevent injury or loss of life

6. The IGA commits parties to the agreement to preserve or introduce legislation as appropriate to the extent necessary to support the collection, use and disclosure of facial images and related identity information via the services.

7. The Bill will amend the Passports Act to ensure that there will be a clear legal basis for DFAT to participate fully in the services. It will do so by adding a new purpose for disclosing information (namely to participate in a service, of a kind specified in a Minister's determination, to a person specified in a Minister's determination, to share or match information relating to the identity of an individual) and providing that the Minister may arrange for the use of computer programs to make decisions.

8. Consistent with provisions in Commonwealth legislation for comparable client-service activities, the Bill will also incorporate scope for the Minister to automate other decisions under the Passports Act. The intention is that these be low-risk decisions that a computer can make within objective parameters, such as decisions to collect personal information for processing passport applications using the FVS and decisions to issue passports to people whose biographical data and facial images exactly match information in previous passport applications.

9. The Bill further provides that decisions made by a computer may be substituted if found to be incorrect, and that this does not limit the reviewability of decisions about Australian travel documents.

Financial impact statement

10. The measures in the Bill do not have any associated cost.

STATEMENT OF COMPATABILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Australian Passports Amendment (Identity-matching Services) Bill 2018

11. This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Human rights implications

12. The Bill engages the following rights:

- protection against arbitrary or unlawful interference with privacy contained in Article 17 of the International Covenant on Civil and Political Rights (ICCPR)
- the right to liberty and security of the person contained in Article 9 of the ICCPR

The right to privacy – Article 17 of the ICCPR

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

14. The right to privacy articulated in Article 17 of the ICCPR may be subject to permissible limitations that are authorised by law, are not arbitrary, pursue a legitimate objective, are necessary to achieve that objective, and are a proportionate means of achieving it. In order for an interference with the right to privacy not to be arbitrary, the interference must be for a reason consistent with the provisions, aims and objectives of the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights Committee (the UNHRC) has interpreted 'reasonableness' in this context to mean that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.

15. The Bill engages and limits the right to privacy because it inserts into the *Australian Passports Act 2005* (the Passports Act) an additional purpose for the disclosure of personal information by the Minister, specifically for participating in a service to share or match information relating to the identity of a person. This personal information will include data page information, status information, request information and authenticity information. These types of information include, for example, biographic details such as names, dates of birth, and gender, as well as facial images.

16. These amendments to the Passports Act will enable the Minister to authorise the Department of Foreign Affairs and Trade (DFAT) to participate fully in the identity-matching services to which the Commonwealth and the States and Territories agreed in the *Intergovernmental Agreement on Identity Matching Services* (IGA), signed at a meeting of the Council of Australian Governments on 5 October 2017.

17. The identity-matching services will facilitate the secure, automated and accountable exchange of identity information between Commonwealth and state and territory governments on a query and response basis, without storing any personal information.

18. The IGA identifies the purposes of the services as: preventing identity crime; general law enforcement; national security; protective security; community safety; road safety; and identity verification. These are also the purposes of the measures in the Bill which provide for DFAT's participation in the services.

19. Robust identity-checking practices have significant benefits for individuals and for the community. They help to secure the legitimate identities of individuals by enabling agencies and organisations to detect and prevent the use of stolen, fake or fraudulent identity documentation.

20. The use of fraudulent identities is also a key enabler of organised crime and 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.

21. In addition to combating identity and related crimes, there are a range of other situations in which identity verification is essential to law enforcement, national security and community safety. This may include verifying the identity of a person suspected of committing a criminal offence, a person seeking authorisation to access a government facility, or a person who is believed to be a missing person. In circumstances such as these, there is a clear need to be able to verify the person's identity in order to protect the community or the individual themselves.

22. By enabling DFAT to share information via the identity matching services, the Bill is pursuing the legitimate objective of making fast and secure identity verification available to support a range of identity-check processes. These processes protect individuals and the community from identity crime and other harms.

23. Sharing personal information through the services is reasonable and necessary to achieve these objectives, and will be designed to ensure that its privacy implications are proportionate to the needs of those services for specific activities.

24. The services will provide a fast and secure tool for identity verification by government and non-government authorities in support of the legitimate objectives of combatting identity crime and supporting national security, law enforcement and community safety. DFAT's participation in the services are necessary to support these objectives because current identity verification practices are inadequate to deal with sophisticated fraudulent identity documents, and to support fast, secure and auditable information-sharing.

25. Where national security or law enforcement agencies have information about potential threats, it is essential that they can act quickly and efficiently to assess the nature of the threat, including identifying any individuals involved. This is particularly important where agencies may not have sufficient information about the known identity of the individual to verify their identity using the services. This may

occur where the agency has a facial image of a suspect but no other identification information about the individual.

26. There is a clear need for government and private sector service providers to improve their identity-verification processes to ensure they can continue to detect these increasingly sophisticated fraudulent identity documents. The services, and DFAT's participation, will assist with this by ensuring that the use of a wider range of fraudulent identification documents can be prevented in a fast, automated and secure way.

27. Many agencies and organisations already have data-sharing arrangements for the purpose of manual facial matching. However, these arrangements can be ad-hoc, often relying on manual processes, may not be secure and may be difficult to audit. By contrast, the services will be delivered through an interoperability hub. The hub will capture audit trail information of all services, to support accountability and transparency measures including regular audits and annual reporting.

28. The services, and DFAT's participation, will help ensure that identity verification processes are able to match the increasing sophistication of fraudulent identity document production, and to support fast, secure and auditable information-sharing. Given the importance of the objectives of the services in relation to reducing identity and related crime and supporting national security, law enforcement and community safety, the imposition on privacy as a result of the services, and DFAT's participation in the services, is reasonable to achieve these objectives.

29. Policy and administrative privacy safeguards including requirements for privacy impact assessments before agencies access the services and compliance audits will also help to ensure the use of the services remains proportionate to the need, and prevent any misuse of identification information.

30. The availability of the services for these purposes recognises the increased need to identify unknown individuals in these circumstances in a timely way, to limit the risk of harm to the community as a result of failure to identify an individual.

31. The risk of harm arising from these types of situations justifies the imposition on the privacy of individuals that DFAT sharing information via the services involves.

32. The principle governing these arrangements is that the minimum necessary information is disclosed to meet the legitimate purpose of the services. The IGA provides that strict privacy controls, accountability and transparency must apply to all the services. Within this framework, data-holding agencies retain discretion to determine specific purposes for which, entities to which, and other circumstances under which, they make their data available through the services.

33. These and other privacy, accountability and transparency measures provide appropriate safeguards against unnecessary impositions on the right to privacy as a result of the Minister making Australian travel document data available for all the purposes of, and by the automated means intrinsic to, the services.

The right to liberty and physical security - Article 9 of the ICCPR

34. Article 9 of the ICCPR requires states to provide reasonable and appropriate measures to protect a person's liberty and physical security.

35. The Bill engages Article 9 of the ICCPR by providing a legal basis for ensuring that the Minister is able to make Australian travel document data available for all purposes of identity-matching services, not just purposes authorised by other provisions of the Passport Act or by other legislation, such as the *Privacy Act 1988*, and that this data may be made disclosed by means of decisions made by a computer.

36. These amendments to the Passports Act will enable the Minister to authorise DFAT to participate fully in the automated matching services to which the Commonwealth and the States and Territories agreed in the *Intergovernmental Agreement on Identity Matching Services* (IGA), signed at a meeting of the Council of Australian Governments on 5 October 2017.

37. The IGA identifies the purposes of the services as: preventing identity crime; general law enforcement; national security; protective security; community safety; road safety; and identity verification. These purposes are directly relevant to the liberty and physical security of individuals in the community.

38. The services will be automated because the expected volume of transactions will preclude human intervention, and because automating disclosures will allow law enforcement and national security agencies to act without delay to identify people in circumstances where their liberty and physical security, or the liberty and physical security of others, are under threat, and take time-critical action to prevent injury or loss of life. Knowledge of the timely availability of Australian travel document data via identity-matching services is also intended to serve as a deterrent to persons who may otherwise commit criminal offences, especially offences that directly or indirectly involve identity crime.

39. By ensuring a legal basis for Australian travel document data to be provided on an automated basis to assist in preventing and detecting identity crime, the Bill will reduce the impact of identity crime in the community. Identity crime imposes significant economic costs through fraudulent financial and commercial transactions and facilitates terrorist, narcotics and money-laundering offences. By making fraudulent identities more difficult to obtain and to use, and by improving the ability of law enforcement agencies to detect fraudulent identities in a timely manner, the Bill will help reduce such negative impacts on personal liberty.

Conclusion

40. The Bill is compatible with human rights because it promotes the safety and security of persons in the community. To the extent that it may limit human rights, particularly the right to privacy, any such limitations are reasonable, necessary and proportionate to achieving that objective.

41. In aiming to promote identity security, minimise the impact of identity-related crime on innocent individuals, and protect individuals from national security, criminal, and road safety threats, the Bill is consistent with the provisions, aims and objectives of the ICCPR.

NOTES ON CLAUSES

Part 1—Preliminary

Clause 1—Short Title

1. Clause 1 is a formal provision specifying the short title of the Bill which, when enacted, is to be cited as the *Australian Passports Amendment (Identity-matching Services) Act 2018*.

Clause 2—Commencement

2. Clause 2 provides that the Act will commence the day after it receives the Royal Assent.

Clause 3—Schedules

3. Clause 3 provides that legislation specified in a Schedule to the Act is to be amended or repealed as set out in the applicable items in the Schedule concerned, and stipulates that any other item in a Schedule to the Act has effect according to its terms.

Schedule 1—Amendments to the *Australian Passports Act 2005*

Item 1 – After paragraph 46(d)

4. Item 1 inserts by means of a new subsection 46(da) an additional purpose for the disclosure of personal information by the Minister, of a kind specified in a Minister's determination, to a person specified in a Minister's determination.

5. Specifically, the new subsection provides that the Minister may disclose personal information for the purpose of participating in a service, specified or of a kind specified in a Minister's determination, to share or match information relating to the identity of a person.

6. By making such a determination, the Minister will be able to authorise the disclosure of personal information via an identity-matching service for all the purposes of that service rather than just for purposes already set out in other parts of section 46 or in other legislation, such as the *Privacy Act 1988*.

Item 2 – Application of amendments

7. Item 2 specifies that the amendments to section 46 made by this Schedule apply in relation to any information disclosed after the commencement of this item (whether the information was obtained before or after that commencement).

8. The effect is that the Minister will be able to authorise the disclosure of any relevant personal information that it has on record, not just information collected after the commencement of the item.

Item 3 – After section 56

9. Item 3 inserts new section 56A, which provides that the Minister may arrange for use, under the Minister's control, of computer programs for making decisions, exercising power or complying with obligations made for the purposes of the Act. For

the purposes of this Act or the legislative instrument, the Minister is taken to have made a decision, exercised a power or complied with an obligation that was made, exercised or complied with or done by the operation of a computer program.

10. This provision will allow the Minister to arrange automated disclosures of personal information for the purposes of the new subsection 46(da) inserted by this Schedule. This is necessary to facilitate DFAT's full participation in the services, given that they will operate on an automated basis.

11. This provision is not limited to decisions about the disclosure of personal information. Consistent with provisions in Commonwealth legislation for comparable client-service activities, it will also give scope for the Minister to arrange the automation of other decisions under the Passports Act.

12. The intention is that these be low-risk decisions that a computer can make within objective parameters, such as decisions to collect personal information for processing passport applications using the Face Verification Service, and decisions to issue passports to people whose biographical data and facial images match previous passport applications.

13. Item 3 further provides that decisions made by a computer can be substituted if found to be incorrect, and that this does not limit the reviewability of decisions about Australian travel documents.

Item 4 – Application of amendments

14. Item 4 specifies that Section 56A of the Passports Act, as inserted by this Schedule, applies in relation to anything done after the commencement of this item.