Australian Government
Department of Foreign Affairs and Trade

AUSTRALIAN PASSPORT OFFICE

Parliamentary Joint Committee on Intelligence and Security

Inquiry into the *Australian Passports Amendment (Identity-matching Services) Bill 2018*

Submission by the
Department of Foreign Affairs and Trade
April 2018

Table of contents

Introduction

1. The Department of Foreign Affairs and Trade (the Department) provides this submission to assist the Parliamentary Joint Committee on Intelligence and Security (the Committee) in its review of the *Australian Passports Amendment (Identity-matching Services) Bill 2018* (the Bill).

Overview of submission

2. This submission complements the Explanatory Memorandum by providing additional information to assist the Committee in understanding aspects of the Bill related to automated decision-making in which the Committee has expressed particular interest.

3. This submission also addresses issues raised in submissions to the Committee's inquiry and published on the inquiry webpage that relate specifically to the Bill.

4. The Department notes that the Department of Home Affairs has submitted to the Committee information on matters relating to the *Identity-matching Services Bill 2018* (the IMS bill) and the broader identity-matching services framework. The Department refers the Committee to this information where issues relate to that broader framework.

5. The Department understands that further submissions may be received by the Committee and will be available to address any further issues raised in those submissions via an appearance at a public hearing of the inquiry.

Information to assist the Committee in understanding the intention of the Bill

6. The Bill amends the *Australian Passports Act 2005* (the Act) to enable the Minister to make Australian travel document data available for the purposes of, and by the automated means intrinsic to, the identity-matching services to which the Commonwealth, states and territories agreed in the Intergovernmental Agreement on Identity Matching Services (IGA), agreed by COAG on 5 October 2017.

7. Consistent with provisions in Commonwealth legislation for client-service activities in other agencies, the Bill also incorporates scope for the Minister to automate other decisions under the Act. The intention is to allow for the automation of low-risk decisions that a computer program can make within objective parameters.

Examples of automated decision-making envisaged under the Bill

8. In a communication on Friday 13 April, the Committee invited the Department to provide three examples of the types of automated decision-making envisaged under the Bill – including an explanation of how those decisions are currently made and how they would be made differently under the Bill.

Decisions to disclose personal information

9. The Department currently provides a service that discloses biometric information about passport holders to Commonwealth and State and Territory agencies in ways analogous to the Face Verification Service (FVS) and Face Identification Service (FIS).

10. The service is manual. Requests are ad hoc. A person in another agency will send an email to an inbox in the Department seeking to:

    a. verify that a person presenting as the holder of a travel document is the person to whom that document was issued

    b. verify travel document information about a person whose image the other agency holds

    c. obtain travel document information about a person whose image the other agency holds.

11. The Department is willing in principle to process requests for any disclosure authorised by the Act or the *Privacy Act 1988*, but in practice all biometric requests are made under Australian Privacy Principle 6.2(e), that is, for enforcement-related activities.

12. The requesting email attaches a completed request form that can also be used for requesting non-biometric disclosures (for instance requests to verify that a physical document has not been tampered with). The requestor must state the reason for the request. Emails making biometric requests also include or attach an electronic facial image.

13. The Department only accepts requests from an official Australian Commonwealth or State or Territory government email address. The sender must assert that they have responsibility within that agency for the matter of the request. If these assertions seem out of place, the Department will query them. One agency – the Child Support Division in the Department of Human Services – has provided a list of staff authorised to make such requests.

14. The desk-level staff member who manages the in-box decides to make the disclosure. This decision is made on the basis of a formal delegation under the Act. The process involves conducting a simple check to ensure that the requesting information satisfies the above requirements and to obtain any missing information. The staff member then interrogates departmental systems to obtain the personal information of the subject of the request. The staff member may need to seek some of that from departmental colleagues by email. Once the personal information has been gathered and is ready, the staff member discloses it by email to the requestor. The staff member archives the paperwork in individual records.

15. The Department does not have the specialist law enforcement expertise needed to assess the merits of the requests it receives, and does not seek information on this from other agencies. As such, its decisions about whether to disclose personal information to these agencies are, in a sense, mechanistic, based on whether requests satisfy simple business rules. If agencies satisfy those conditions, the Department will in practice always approve their requests.

16. The manual nature of this operation has a number of drawbacks. It is labour-intensive, slow and only able to process small volumes of requests. Although the Department would be glad to use this service to conduct routine, consent-based biometric identity checks to confirm identity in situations unrelated to law enforcement, these practical drawbacks mean that such checks do not happen.

17. The Department has no case management system of its own to keep track of the progress of requests. Absent such a system, there are no biometric request audit logs. There is also no database of biometric requests that could be interrogated for the purpose for generating statistics, production of which would require extensive and unreliable manual cross-checking.

18. The service is workable only because of the low volumes. In the absence of reliable statistics, the Department estimates that it processes up to a few *hundred* biometric requests to disclose information every *year* for purposes comparable to those of the FVS and FIS. Once the FVS is in in full swing, the Department is likely to receive *thousands* of disclosure requests per *day* via that service.

19. The automation intrinsic to the FVS and FIS has been designed to overcome limitations such as those of DFAT's current service. The new systems will be fast, with the Department's FVS designed to provide results within a few seconds. The FVS in particular will be able to handle high volumes. Requests will come in via a secure hub rather than by email. There will be an extensive audit and statistical capability to ensure that users are authorised by their agencies to have access to the services and that they only use this access for prescribed purposes consistent with privacy requirements. User constraints will be especially tight for the FIS. Business rules will be incorporated into the interfaces used by requestors so that requests are always within the required parameters and always include the minimum required information.

20. Automated passport information disclosure through the FVS and FIS will produce benefits that the Department's current, manual disclosure service cannot provide. The new services will help law enforcement and national security agencies to act without delay and take time-critical action where needed to prevent injury or loss of life, for example in a terrorist scenario similar to the Lindt Cafe siege. The new services will assist persons undertaking legitimate transactions with government agencies. They will help to secure the legitimate identities of individuals by enabling agencies to detect and prevent the use of stolen, fake or fraudulent identity documentation.

21. There is one important sense – beneficial to the rights of individuals – in which the FVS and the FIS will have *less* functionality than the Department's current service. Under the current service, the Department can *negatively identify* a subject by disclosing personal biometric information that is legally prejudicial, such as by providing an opinion that the subject is not the valid holder of a claimed travel document, or that a passport holder matches the image of the suspect in a criminal investigation. The FVS and FIS will not make such negative disclosures.

22. The FVS is designed to *positively* identify a subject. The user will provide biographic details about the subject (such as their name and date of birth), which will then be checked against any existing passport records for that individual. Biometric results will only be returned if the biographic details match a record. Where the biographic or biometric data do not match, the user will receive a message to this effect. There could be a number of possible reasons for a 'no match' message, such as poor photo quality or errors in how the user has entered the biographical data. Users will be able to resubmit requests to resolve such issues. Where a match cannot be confirmed via the automated service, it is likely that the requestor will contact the Department to ask that a human operator resolve the discrepancy. The effect of these arrangements is that the Department will have no capacity to use the FVS to disclose that a person is *not* the valid holder of a particular passport. As is currently the case, any such negative disclosure will have to be made manually.

23. The FIS will not of itself *identify* subjects, only generate leads so that humans can make an identification. The user will submit an image of an unknown person. The Department's systems will generate a number of potential matches and disclose them automatically. Unlike under its current service, the Department will *not*, as part of that operation, disclose an opinion on whether any of those images actually do match the subject. The requestor will form an opinion on that manually.

Decisions to collect personal information

24. Automating decisions to collect information through the FVS during the passport issuing process could further strengthen the integrity and security of the Australian passport.

25. For instance, the Department might add functionality to its internal passport processing software so that it could use the FVS to initiate routine biometric verification of driver licence images in respect of all passport applicants. At present, given the current capabilities of the FVS, the Department only undertakes manual biometric driver licence image checks, and only then if there is an indication of fraud. The process for making these decisions is that a human operator determines that a check is needed and sends an email to the relevant driver licence authority. Utilising the new capabilities of the FVS to automate this kind of collection on a routine basis could further enhance the integrity of passport issuing processes.

26. As in the case of disclosures, the Department would only collect information automatically for the purpose of *positively verifying identity*. Where the biometric information provided with a passport application matched the driver licence information for that identity, processing would proceed with no need for manual evaluation. Where a match could not be confirmed, the discrepancy would be referred for manual evaluation by a human passport officer.

Decisions to issue passports

27. The Department envisages automating decisions to issue passports to certain low-risk categories of applicants.

28. The principal group the Department has in mind are known adult clients who submit applications containing biographical data and facial images that match information held on record in the Department from previous passport applications.

29. Currently, if an adult applicant has held a passport previously (that is, if the application is a renewal application), the Department's passport processing software compares the client's biographical data and image to records of all applicants in the Department's database to check that the applicant is applying in the same identity as their previous passport and that no other identities are associated with that facial image. The system also carries out other routine checks against business rules, for instance to ensure that there is no alert in the passport system related to law enforcement or security. If biographical data, facial image and other checks generate any anomalies, the Department's passport processing software generates an 'assessment' in respect of each anomaly. An 'assessment' in this context is a manual task that a processing officer will need to carry out to resolve an issue in an application.

30. Most of the roughly 4,500 adult renewal applications the Department processes every day generate no assessments. That is, they match the records of known clients, consistent with business rules, with no discrepancies. As such, the Department's systems and procedures do not require processing officers to undertake any manual checks. All of these applications are presented to processing officers anyway. The only task for the processing officers is to authorise the issue of the passports. The Bill's insertion of Section 56A into the Act would enable the Minister to arrange for the Department to automate that task. This would allow processing officers to devote their attention to renewals that *do* generate assessments, and which are therefore likely to involve more risk. It would also mean that renewal applicants would receive their new passports sooner. Given that renewal applications comprise 55 per cent of the passport caseload, the potential for benefits is significant.

31. The Department has no, and has no interest in developing, software that would be capable of even recommending, let alone deciding, that an applicant should *not* be issued a passport. Such cases are rare. The Department issued 2,087,288 passports in calendar 2017 but refused only 170 on grounds of suspicion of fraud or dishonesty and refused or cancelled only 70 on national security or law enforcement grounds. The circumstances of all such cases are unique, requiring fine judgment. Decisions on them will always need to be made by a human. The Department's passport processing software directs such cases to a human in every instance.

Issues raised in submissions

32. The Department has carefully considered issues raised in submissions to the Committee.

33. The Department notes that information the Committee has received from the Department of Home Affairs is relevant to issues that other submissions have raised in relation to the IMS Bill and the identity-matching services framework as a whole. The Department will therefore focus its attention in this submission on issues that relate specifically to the Passport Bill.

34. Submissions have raised passport-specific concerns relating to:

- Automated decision-making
- Delegated legislation
- Consent and freedom of movement
- Privacy

35. This submission addresses each of these below.

Concerns relating to automated decision-making

Nature of the concerns

36. A number of submissions[1] express concern about governments using computer programs to make decisions. Among other things, these submissions argue that automation of discretionary decisions amounts to a dereliction of duty on the part of decision-makers[2], that it violates the legal rights of individuals, and that decisions made automatically may be, for that reason, unlawful[3]. Some submissions noted the need to consider community values and to apply concepts such as procedural fairness and common sense in decision-making[4].

37. One of these submissions[5] argues that the Bill may have an adverse impact upon the right of equal access to public service in Article 25 of the International Covenant on Civil and Political Rights (ICCPR) and to equality before the law and equal protection of the law under Article 26 of the ICCPR.

38. Another submission[6] argues the Bill should be amended to ensure that individuals always have the right to request a human make a decision that affects their legal rights and obligations. Two submissions[7] cite Centrelink 'Robodebt' as an example of significant harm that can accrue to individuals as the result of poor decisions by computers.

39. One of the submissions[8] argues that it is difficult to identify how it is that, or whether or not, a computer has made a wrong decision and that the Bill itself, in the proposed paragraph 56A(3)

[1] Submission 2 (Australian Lawyers for Human Rights), Submission 5 (Civil Liberties Australia),Submission 9 (Joint councils for civil liberties)
[2] Submission 2 (Australian Lawyers for Human Rights, at 2.4 and 6.9)
[3] Submission 2 (Australian Lawyers for Human Rights, at 6.10)
[4] Submission 2 (Australian Lawyers for Human Rights), Submission 9 (Joint councils for civil liberties)
[5] Submission 2 (Australian Lawyers for Human Rights, at 4.2)
[6] Submission 5 (Civil Liberties Australia)
[7] Submission 2 (Australian Lawyers for Human Rights, at 6.4 and 6.6), Submission 9 (Joint councils for civil liberties, at 46)
[8] Submission 2 (Australian Lawyers for Human Rights, at 2.5, 6.2 and 6.5)

acknowledges the 'fallibility of computer programmes' by allowing decisions by a computer to be substituted if found to be incorrect.

40. Some of the submissions argue that a computer programme will reflect the intrinsic social biases of the programmers[9] and that the underpinning data or criteria used to generate these decisions should be made publicly available[10].

Response from the Department

41. The concerns expressed in the submissions are based on an expectation that the Department intends to use automation to make decisions that may have a negative impact on the subjects of those decisions. This is not the case. As outlined in the examples in the previous section, the Department does not intend this. In fact, given the way that the FVS, the FIS and the Department's passport processing systems are designed, the Department is in practice only *able* to automate decisions that produce favourable or neutral outcomes for the subject. Such decisions would not negatively affect a person's legal rights or obligations, and would thus not generate a reason to seek review.

42. In this context, the practical function of paragraph 56A(3) of the Bill is to make clear, for the avoidance of doubt, that the Minister is able to substitute incorrect automated decisions made *in favour* of a client. If, after a passport were issued automatically, a new piece of information indicated that it should not have been (for instance if the applicant was discovered to have been subject to an undisclosed adult guardianship order – information that a human decision-maker would also not have known about), it would be important that the Minister, acting manually, have the power to correct that decision.

43. Another example of possible computer error would be if a person presented the biographical information of a close relative with their own facial image, and their facial image were similar enough to that of the relative that it generated a false positive match, leading the computer to decide to issue a passport. But most *humans* would be *more likely* than a computer program to get this wrong.

44. The types of outcomes enabled by automated decisions would, in most cases (the bulk of FVS disclosures and all passport renewals), involve comparing two data sets belonging to *same person*. In other cases (some FVS and all FIS disclosures) it would involve *seeking* data that matched the same person. Matching individuals against themselves leaves little scope for social bias. A computer program will in any event generally make decisions with less bias than a human, and any such bias is more easily analysed and corrected than the thought processes of individuals. A computer program will also make decisions more consistently, especially repetitive decisions. And a computer program is far more likely than a human to identify consistently and correctly any discrepancies that require more detailed consideration. That is, a computer is less likely to 'miss something'.

45. Every other Commonwealth and State and Territory Data Holding agency participating in the identity-matching services will do so on the basis of automated disclosures. There is nothing about passport information that would make it uniquely unsuited to this.

[9] Submission 2 (Australian Lawyers for Human Rights, at 6.2)
[10] Submission 9 (Joint councils for civil liberties, at 47)

Concerns relating to delegated legislation

Nature of the concerns

46. One submission expressed concern specifically about the use of delegated legislation in the proposed new paragraph 46(da) of the Act, arguing that rules affecting individual rights should be in primary legislation. That submission recommended that paragraph 46(da) be amended to specify that provisions impacting individual rights and liberties should be included in the Act.[11]

Response from the Department

47. Section 46 of the Act lists particular purposes for which personal information may be disclosed under the Act. Section 46 further provides that the kind of personal information disclosed for these purposes, and the persons to whom it may be disclosed, are to be specified in a Minister's determination.

48. Section 46 currently lists five purposes for which personal information may be disclosed:

a) confirming or verifying information relating to an applicant for an Australian travel document or a person to whom an Australian travel document has been issued
b) facilitating or otherwise assisting the international travel of a person to whom an Australian travel document has been issued
c) law enforcement
d) the operation of family law and related matters
e) the purposes of a law of the Commonwealth specified in a Minister's determination.

49. The Australian Passports Determination 2015 (the Determination) specifies in section 23 the kinds of information that may be disclosed for each of these purposes, the persons to whom it may be disclosed and, with regard to paragraph 46(e) of the Act, laws in respect of which it may be disclosed.

50. The matters regulated in section 23 are matters of administration and detail and are subject to frequent technical changes, such as changes to the titles of the agencies and office-holders to whom different disclosures may be made. In enacting the Act, the Parliament considered it appropriate that these matters be regulated through delegated legislation.

51. The Bill will amend the Act to add a new purpose for disclosing information, namely to participate in a service to share or match information relating to the identity of an individual. It is appropriate, and consistent with the general operation of the Act, that this new purpose be inserted into the list in section 46, and that, by normal operation of that section, details about the kinds of information that may be disclosed, the persons to whom it may be disclosed, and the services or kinds of service by which such disclosures may be made, be specified in the Determination. The Determination is a transparent and publically available instrument. Amendments to the Determination are tabled in Parliament for a disallowable period.

[11] Submission 9 (Joint councils for civil liberties, recommendation 9)

Concerns relating to freedom of movement

Nature of the concerns

52. One submission[12] raises concerns that the Bill would engage rights protected in Article 12 of the International Covenant on Civil and Political Rights, because a person who requires a passport to travel internationally will have to consent to the use of their personal information for identity-matching purposes or their freedom of movement will be restricted.

Response from the Department

53. It is possible to construe the Bill as engaging the right to freedom of movement of people who objected to the use of their data in the identity-matching services. However, to the extent that this is the case, the effect is limited and reasonable.

54. When lodging a passport application, applicants are already required to sign a declaration that they understand their photograph and personal information will be used for data and biometric matching purposes (even if the application is withdrawn). By operation of paragraph 7(3)(a) of the Act, a passport application cannot be processed without signature of this declaration. The provisions in the Bill will not require any expansion of this acknowledgement.

55. The Statement of Compatibility with Human Rights in the Explanatory Memorandum to the Bill sets out why it is reasonable for the Minister to make Australian travel document data available for all the purposes of, and by the automated means intrinsic to, the identity-matching services and how the design, governance and transparency of the services provide appropriate safeguards against unnecessary impositions on the right to privacy. These considerations apply *mutatis mutandis* to any engagement of the right to freedom of movement.

Concerns relating to privacy

Nature of the concerns

56. Five submissions that raise privacy concerns related to the identity-matching services also make specific reference to the Passport Bill. Two of these[13] raise issues relating to the right to privacy. The other three[14] raise issues relating to consent to the (secondary or tertiary) use of passport data, including by arguing that the original consent obtained in the past in relation to the data concerned (for example, a passport photo) does not amount to consent to the kinds of disclosures foreseen in the Bill.

Response from the Department

57. Although these submissions reference the Bill, the concerns they raise are generic to the operation of the identity-matching services rather than unique to passport disclosures.

58. The Department refers to information already provided in the Human Rights Compatibility Statements attached to the Explanatory Memorandums for both Bills, and to information provided to the Committee by the Department of Home Affairs. This information sets out the robust privacy, transparency and accountability controls intrinsic to the identity-matching services that address these concerns.

---

[12] Submission 11 (Australian Human Rights Commission, at 48-50)
[13] Submission 2 (Australian Lawyers for Human Rights) and Submission 11 (Australian Human Rights Commission)
[14] Submission 1 (Future Wise and the Australian Privacy Foundation), Submission 5 (Civil Liberties Australia), Submission 8 (Law Council of Australia, at 12)

Concluding remarks

59. The Department's participation in the identity-matching services will help to strengthen the integrity and security of Australia's identity infrastructure—including the security of Australian passports, one of the most trusted identity documents in the world.

60. By enabling the Department to automate low-risk decisions that a computer can make within objective parameters, resulting in faster, more reliable, positive or neutral outcomes for clients, the Bill will allow passport processing officers to focus on more complex, high-risk decision-making, further enhancing passport security.

61. The Department thanks the Committee for the opportunity to address its questions, and to consider and respond to other submissions the Committee has received.