Australian Government
Department of Home Affairs

May 2018

# Parliamentary Joint Committee on Intelligence and Security

## Department of Home Affairs
## Supplementary Submission

## Inquiry into the Identity-matching Services Bill 2018

# Table of Contents

# Introduction

1. The Department of Home Affairs (the Department) provides this supplementary submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee's) inquiry into the Identity-matching Services Bill 2018 (the Bill), in addition to its first submission provided to the Committee on 11 April 2018.

## Overview of submission

2. This supplementary submission addresses issues raised in submissions to the inquiry made by entities other than the Department and published on the inquiry webpage, where those issues are not already addressed in the Department's first submission.

3. 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.

4. This supplementary submission does not deal with issues relating the Australian Passports Amendment (Identity-matching Services) Bill 2018, which is also being considered by the Committee as part of this inquiry.

5. The Department refers the Committee to the Department's first submission for a description of the purpose and effect of the Bill.

# Issues raised in submissions

6. The Department has raised in submissions referred to in paragraph 2 above. The issues raised in the submissions relate to the following:

   - Consent and notification – concerning the requirements for a person to consent to use of their personal information for the provision of the identity-matching services
   - Oversight of the identity-matching services
   - Private sector use of verification services
   - Proportionality and scope of measures in the Bill
   - Rule-making powers in the Bill
   - Security and accuracy issues in relation to use of the identity-matching services.

7. This submission will address each of these below.

8. On a preliminary note, a number of submissions are predicated on a misconception that the Bill authorises agencies participating in the services (other than the Department) to collect, use or disclose identification information.

9. As noted in the Department's first submission and by the Minister in his second reading speech, the Bill does not authorise any agency other than the Department to collect, use or disclose identification information via the services. The Bill does not seek to expand the legal authorisation that other agencies have to share identification information through the services or otherwise. It simply provides the Department with the authorisation it requires, subject to appropriate safeguards, to operate the technical systems that will facilitate information-sharing via the services in a more efficient, secure and, accountable way than other existing arrangements.

10. The definitional clauses in the Bill are intended to impose appropriate restrictions on this authorisation so as to ensure the Department can only operate the services for the purposes for which data-holding agencies have broadly agreed to share information in accordance with the *Intergovernmental Agreement on Identity Matching Services* (IGA) agreed by COAG in October 2017. Data-holding agencies retain control over the information they will share with other agencies, and the purposes for which they will share it, within the confines of their legal authority to do so. This approach has been taken to avoid providing a blanket authorisation for all users of the services, ensuring that information-sharing through the services is subject to appropriate jurisdiction, function, or agency-specific authorisations and protections.

11. The data sources that will be available for matching through the services already exist and are accessed by various agencies for a range of purposes under existing data-sharing arrangements, in accordance with applicable legislation. Concerns about these data sources, or the purposes for which they are held and shared, would be more appropriately addressed through separate processes.

## Consent and notification

12. A number of submissions to the inquiry raise concerns relating to the issue of how a person may give consent to the use of their personal information in the provision of an identity-matching service.

*Genuine consent*

13. The first consent-related issue raised in submissions relates to how a person can genuinely consent to the use of their identification information in the services.

14. In summary, the submissions argue that a person may not be able to give genuine consent to their identification information being used to verify their identity using an identity-matching service. It is argued that a person who requires an important or essential service, such as the provision of a driver licence, may not have a genuine choice to decline to have their identity verified through a face-matching service.[1]

15. This issue is raised particularly in relation to the Face Verification Service (FVS). The FVS is an identity-matching service that assists government agencies and private sector organisations to verify a known or claimed identity against government identification documentation. Clause 10 of the Bill sets out the operation of the FVS. Further information about the FVS can be found in paragraphs 139-155 of the Explanatory Memorandum to the Bill (the EM).

16. Under the Bill, both government agencies and private sector organisations may potentially use the FVS. Under clause 10(2) of the Bill, any entity that wishes to use the FVS must have a legal basis to collect, use or disclose identification information. For Commonwealth, state and territory government users of the FVS, consent is only one of a number of legal bases that agencies may rely on to use the FVS. For private sector and local government users of the FVS, which were a focus in the submissions that addressed consent issues, paragraph 7(3)(b) of the Bill specifically provides that consent of the individual whose identity is being verified is required in all cases.

17. The concept of 'consent' in the Bill is based on relevant provisions of the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Privacy Act), and comparable state and territory privacy legislation.[2] APP 3.3(a) permits an APP entity to collect sensitive information about an individual with that person's consent, where it is reasonably necessary for the entity's functions. In addition APP 6.1(a) permits an APP entity to use or disclose personal information about an individual for a secondary purpose with that person's consent. Paragraphs 231-233 of the EM further explain how the concept of 'consent' is intended to be interpreted in the Bill.

18. The Office of the Australian Information Commissioner's *Australian Privacy Principles Guidelines* (APP Guidelines) set out the requirements for 'consent' as follows:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily

[1] Submission 1, Future Wise and the Australian Privacy Foundation, section 6, p. 10; Submission 2, Australian Lawyers for Human Rights, paras 5.14-15; Submission 8, Law Council of Australia, para 8; Submission 8.1, Law Council of Australia, paras 11-13, 104, 124(b).
[2] A list of state and territory privacy legislation appears in para 117 of the EM.

- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

19. The obtaining of consent for use of the FVS will operate in the same way as it does in the context of the existing Document Verification Service (DVS). Established under the *Intergovernmental Agreement to a National Identity Security Strategy* of 2007, the DVS enables government and non-government users to compare information on government identification documents with a corresponding government record to help verify a person's identity. The DVS matches key biographic details about the individual and their Australia-issued identifying credentials (such as a passport or driver licence), and provides a 'yes' or 'no' match response.

20. The DVS relies on its private sector users meeting the consent and other privacy requirements referred to in the APP Guidelines.[3] There are regular audits to ensure users are meeting their obligations in relation to their use of the services, including consent requirements. The Department will also publish information about the services on a website, similar to that contained on the DVS website[4], to help individuals understand how their information is collected and used through the services.

21. Under the IGA, which sets out the agreement between the Commonwealth and the states and territories on the provision of the identity-matching services, private sector access to the FVS to match against state and territory data would also be subject to the outcomes of privacy impact assessments on each type of organisation that will use the services, and an FVS Commercial Service Access Policy including an audit and compliance programme. These processes will consider processes for obtaining consent, and provide an opportunity to identify any non-compliance with consent obligations.

22. However, nothing in the Bill mandates the use of the FVS by private sector organisations, contrary to what is claimed in one submission.[5] Any use of the FVS by the private sector will be on an opt-in basis, and user organisations will need to ensure that they meet their obligations under the Privacy Act, and other legislation that applies to them, including to obtain genuine consent from their customers in relation to the use of their identification information in an FVS check. This may mean, for example, providing alternative options for identity verification using the DVS or other identity verification processes if a customer does not consent to the use of their identification information through the FVS. As is currently the case for the private sector's use of DVS, the Department's future audit activities would focus on ensuring that consent was properly captured for use of the FVS.

23. In the same context, some submissions raise concerns that the Bill may affect the provision in APP 2 for anonymity or pseudonymity in dealing with an APP entity.[6]

24. However, as the submissions themselves note, the APPs contemplate circumstances in which the right to anonymity or pseudonymity does not apply. These include circumstances where an entity is required or authorised by law to deal with individuals who have identified themselves or where it is impracticable for the agency to deal with individuals who have not identified

[3] See https://www.dvs.gov.au/How-the-DVS-works/Pages/The-DVS-and-consent.aspx.
[4] www.dvs.gov.au
[5] Submission 1, Future Wise and the Australian Privacy Foundation, section 6
[6] Submission 2, Australian Lawyers for Human Rights, paras 5.12-13; Submission 9, Joint Councils of Civil L berties, paras 29-31.

themselves. It is not possible for the Department to provide identity-matching services without access to identifying information.

25. As mentioned above, other entities using the identity-matching services will need to comply with all privacy protections that apply to them. For those subject to the APPs this includes the requirement to provide for anonymity or pseudonymity unless the entity meets one of the exemptions in APP 2.

*Consent for secondary usage and notification*

26. The second consent-related issue raised in submissions relates to whether persons who have consented to use of their identification information for the provision of an identity document (such as a driver licence or passport), have also consented to the secondary use of their identification information in the identity-matching services.[7] One submission argues that secondary usage of personal information for the identity-matching services should only be permitted with the consent of the relevant individual.[8]

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

28. APP 6 permits the use or disclosure of personal information for secondary purposes without consent in certain circumstances. These include where the disclosure is: authorised or required under an Australian law or court/tribunal order (APP 6.2(b)); or for enforcement related activities conducted by or on behalf of an enforcement body (APP 6.2(e)).

29. In its role facilitating the identity-matching services, as the operator of the interoperability hub and the National Driver Licence Facial Recognition Solution (NDLFRS), the Department does not interact directly with individuals whose information is used in the services. These interactions are conducted by the agencies which seek to use the services and/or the data-holding agencies which make their information available via the services. Therefore it is impracticable for the Department to collect consent directly from individuals for the secondary use of their information in the identity-matching services.

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

31. Under the IGA, all information-sharing through the services will also be subject to the separate legal basis that each participating agency (i.e. the agency using the service, and the data-holding agency that owns the data used in the response) has to collect, use and disclose identification information, and any legislative restrictions that apply to those activities including under the Privacy Act or other applicable privacy legislation. This means that data-holding agencies who collect information for one purpose (such as road agencies collecting information in order to issue driver licences), must also have a legal basis to share that

[7] Submission 1, Future Wise and the Australian Privacy Foundation, section 6; Submission 2, Australian Lawyers for Human Rights, para 5.2; Submission 5, Civil L berties Australia, p. 2; Submission 8, Law Council of Australia, para 12; Submission 11, Australian Human Rights Commission, para 12(a).
[8] Submission 2, Australian Lawyers for Human Rights, paras 5.2-3.

information through the identity-matching services, whether based on consent or another legislative permission.

32. In most cases, data-holding agencies already have legislative permissions to share identification information without the consent of the individual for some or all of the activities for which the identity-matching services will be available. For example, information-sharing for law enforcement purposes already occurs under a range of legislation. It would be impractical for data-holding agencies to rely on a person's consent in order to make their identification information available via the face-matching services in all cases – and particularly for the inclusion of their information in the NDLFRS. To do so would effectively provide criminals with the ability to 'opt-out' of their information being made available to law enforcement agencies that are investigating criminal offences, or allow people using fraudulent identity documents to avoid detection.

33. In addition to legislative protections that apply to all agencies participating in the services, the Department will also make publicly available information on the operation of the identity-matching services so that the community is aware of and can understand how their information is used through these services.

*Notification*

34. Two submissions note that there is no requirement in the Bill to notify persons about the use of their identification information in the identity-matching services.[9]

35. APP 5 already contains a general requirement for APP entities to notify individuals about the collection of their personal information and how that information is used. This requirement will apply to the Department in its operation of the NDLFRS and the provision of identity-matching services facilitated through the interoperability hub.

36. It is not practical for the Department to make this notification directly to individuals because the Department is not collecting information directly from individuals in its role as operator of the interoperability hub and NDLFRS. As such, notification to individuals will rely to a significant extent on data-holding agencies, including state and territory road agencies, to inform individuals about the intended use of their information in the identity-matching services. The Department will work closely with these agencies to ensure that these notifications are updated as the services come online for different data sources.

37. The Department will also fulfil its obligations under APP 5 by making publicly available information on the operation of the identity-matching services so that the community can understand how their information is used through these services.

## Oversight and governance

38. A number of submissions raise issues about oversight of the NDLFRS and the identity-matching services more broadly.

39. The Department's first submission discusses the oversight and governance provisions in the Bill, and foreshadows amendments proposed by the Minister to further enhance these

[9] Submission 8.1, Law Council of Australia, paras 14-15; Submission 9, Joint Councils of Civil Liberties, para 27.

provisions in response to comments made by the Senate Standing Committee for the Scrutiny of Bills in its *Scrutiny Digest No. 2 of 2018*. [10]

40. In summary, the key oversight mechanisms contained in the Bill are:

- Public annual reporting on use of the identity-matching services (clause 28)
- A statutory review of the identity-matching services commencing within five years (clause 29)
- Consultation with the Information Commissioner and the Human Rights Commissioner in the making of certain rules by the Minister (clauses 5(4) (b), 7(5)).

*Biometrics Commissioner*

41. Some submissions suggest the government should establish a Biometrics Commissioner, similar to that established in the United Kingdom in 2016.[11]

42. Whilst the decision about whether to establish such an office would be a matter for government, the Department notes that the role of the UK Office of the Biometrics Commissioner primarily relates to review the retention and use by the police of DNA samples, profiles and fingerprints, and police use of facial biometrics. The Bill is not seeking to expand the circumstances in which police can collect biometric information from individuals, or govern their use or retention of biometric information. The Bill will enable the Department to facilitate information-sharing between agencies that already have a legal basis to do so. The extent to which existing or new police powers in relation to biometric information require greater oversight is a separate issue, outside the scope of the Bill.

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

*Annual reporting*

44. Some submissions argue that the annual report provided for by clause 28 of the Bill should include further information, such as information about data breaches, security incidents and unauthorised usage or disclosure.[12]

45. The annual reporting provisions in the Bill largely require the provision of statistical information on the use of the identity-matching services. This is intended to provide similar types of public information as are required in the annual reports under the *Surveillance Devices Act 2004* and the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

46. Management of data breaches is governed by the new data breach notification provisions in Part IIIC of the Privacy Act. These provisions will apply to the information held or processed in

[10] Home Affairs, *Submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into Identity-matching Services Bill 2018*, paras 29-33.
[11] Submission 1, Future Wise and the Australian Privacy Foundation, p. 12; Submission 8, Law Council of Australia, para 38; Submission 9, Joint Councils of Civil Liberties, para 9.
[12] Submission 3, Queensland Office of the Information Commissioner, pp. 4-5; Submission 4, Office of the Victorian Information Commissioner, para 6; Submission 13, Office of the Australian Information Commissioner, p. 5.

the NDLFRS and through the identity-matching services. It is not necessary to duplicate data breach reporting by requiring this information to be included in the annual report under the Bill.

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

48. One submission suggests that there should be some level of reporting on the use of the identity-matching services by the Australian Security Intelligence Organisation (ASIO).[13] The Bill excludes ASIO from inclusion in the annual report.[14]

49. ASIO has been excluded from annual reporting requirements in the Bill as public reporting on its use of the identity-matching services may compromise national security. This exclusion is consistent with the TIA Act. Under that Act, the annual report does not include information about ASIO usage of warrants and telecommunications data authorisations. The Department also notes that ASIO is exempt from the operation of the Privacy Act and the *Freedom of Information Act 1982* (FOI Act), for similar reasons.

50. ASIO will continue to be subject to its existing oversight regimes, which will apply in relation to ASIO use of the identity-matching services. This includes oversight by the Inspector-General of Intelligence and Security (IGIS).

51. Some submissions also argue that the annual report provisions should require the naming of private sector organisations that use the verification services.[15]

52. The annual reporting provisions of the Bill require general reporting on use of the FVS by private sector users,[16] although this does not extend to naming of specific private sector users. This is consistent with the approach adopted for the DVS over recent years. Many private sector users of the DVS users consider the fact that they use this service should be treated as commercial in confidence information.

*Governance*

53. Some submissions suggest that too many of the core principles, governance arrangements and oversight mechanism for the identity-matching services was are contained in supporting documentation such as agreements and policy documents, and that more of this material should be in the Bill.[17]

---

[13] Submission 8, Law Council of Australia, para 35.
[14] Identity-matching Services Bill 2018, paragraphs 28(1)(a), 28(1)(c)).
[15] Submission 3, Queensland Office of the Information Commissioner, p. 5; Submission 8, Law Council of Australia, para 34.
[16] Identity-matching Services Bill 2018, paragraph 28(b).
[17] Submission 3, Queensland Office of the Information Commissioner, p. 3; Submission 4, Office of the Victorian Information Commissioner, para 1; Submission 13, Office of the Australian Information Commissioner, pp. 3-4.

54. As the Department noted in its first submission, the Bill is not intended to govern the full operation and use of the identity-matching services, which is also subject to the legislation governing the handling of personal information by agencies participating in the services, as users or providers of data. It has been developed to provide an explicit legal basis for the Department's role as the operator of the technical systems that facilitate the services, and to place appropriate safeguards around the operation of those systems and the scope of the identity-matching services that they support.

55. The identity-matching services involve access to both Commonwealth and state and territory data sources. The IGA sets out, in detail, the agreement between the jurisdictions on a range of matters related to the services, including guiding principles, governance and oversight mechanisms. The IGA also provides for certain matters to be managed by agreements made between the parties. This includes, for example, the Face Matching Services Participation Agreement, which sets out terms and conditions, including minimum privacy and security safeguards, for all agencies participating in the services, and the NDLFRS Hosting Agreement, which sets out arrangements for the Department's hosting of state and territory data in the NDLFRS. The matters dealt with in these agreements are subject to negotiation and agreement between Commonwealth, state and territory participants. Fixing this level of detail in legislation may not be appropriate, and may also raise constitutional issues if the legislation seeks to bind state or territory agencies.

56. One submission suggests the Bill should give the Minister the power to decline participation by an agency in the identity-matching services, or to suspend an agency's participation for misuse.[18]

57. The supporting agreements, in particular the Face Matching Services Participation Agreement, manage access to the services and suspension for misuse of the services, which is dealt with administratively (as it is for the DVS). Under the agreements, and pursuant to the IGA, data-holding agencies govern retain full control over decisions on who has access to their information and can direct the suspension of access for a particular user organisation to that information. The Department, as operator of the interoperability hub, can also suspend users for non-compliance with their obligations under the agreements. These decisions will generally be made at the senior officer level in the Department. These decisions will be based, in many cases, on consultation between the Department and affected data-holding and user agencies across more than one jurisdiction. Providing the Minister with administrative powers in relation to the provision of the identity-matching services by the Department would unnecessarily complicate the separation of executive and administrative functions, particularly given state and territory data-holding agencies' role in the system's governance.

58. Another submission notes that the Bill does not contain a requirement for annual audits by the OAIC that are referred to on the Department's website.[19] As noted above, the Bill is not intended to govern the full operation and use of the identity-matching services. The Department has already entered into an MOU with the OAIC to conduct two annual audits in 2017-18 and 2018-19. The Department has funded the OAIC to undertake these audits.

[18] Submission 5, Civil L berties Australia, p. 3.
[19] Submission 8, Law Council of Australia, para 37.

## Private sector use of verification services

59. A number of submissions raise concerns about the provisions in the Bill permitting potential future use of verification services (including the FVS) by the private sector and local government.

60. The Department discussed potential access to the FVS by the private sector and local government in paragraphs 52-60 of its first submission. This supplementary submission addresses issues raised in other submissions that not already covered in the Department's original submission. Issues relating to obtaining consent from individuals for private sector and local government use of the FVS are addressed earlier in this submission.

*No access by the private sector to FIS*

61. One submission raises a concern that the private sector might be given access to the Face Identification Service (FIS) in the future.[20]

62. The FIS is an identity-matching service to assist in ascertaining the identity of unknown persons. More information about the FIS is in paragraphs 120-131 of the EM.

63. Under the Bill, the private sector and local government will only have access to the FVS or another identity *verification* (not identification) service prescribed by the Minister in the rules.[21]

64. Access to the FIS is restricted to the specific list of national security, anti-corruption and law enforcement agencies referred to in clause 8 of the Bill. It will not be possible to prescribe a private sector organisation as having access to the FIS under paragraph 8(2) (q) and subsection 8(3) of the Bill. Under these provisions, only *authorities* that have taken on the functions formerly performed by one of the state or territory authorities listed in paragraphs 8(2) (g) to (p) can be prescribed.

*Legal basis for private sector participation*

65. One submission asserts the Bill does not specify that private sector and local government users must have a legal basis to use the FVS.[22]

66. This statement is incorrect. The requirement for a legal basis to use the FVS appears in clause 10(2) of the Bill. The same submission also asserts that local government may use the services, integrated with CCTV, to issue parking tickets. This is also incorrect, as all local government use requires the consent of the person under paragraph 7(3) (b) of the Bill.

67. Another submission also objects to the possibility that private sector users could use the verification services for the organisation's own service delivery purposes.[23] The submission asserts that the requirement for identity verification to be 'reasonably necessary for an entities' functions or activities' contradicts the objective of providing for private sector access for the purpose of fighting identity crime.

68. The requirement in the Bill for identity verification to be reasonably necessary for the functions or activities of the organisation will operate to prohibit inappropriate usage of the services by private sector and local government users that do not have a need to undertake identity

[20] Submission 4, Office of the Victorian Information Commissioner, paras 4-5.
[21] Identity-matching Services Bill 2018, subclauses 7(2)-(4), 10(2).
[22] Submission 9, Joint Councils of Civil L berties, paras 19-20.
[23] Submission 1, Future Wise and Australian Privacy Foundation, p. 10.

verification in their day-to-day activities. It does not undermine the overall objective in providing access to the FVS to private sector users.

69. Private sector organisations that undertake identity verification as part of their core functions are key partners in detecting and combatting identity crime. They handle a high volume of primary identity documents, and providing access to tools to verify those documents will help to deter and detect the use of fraudulent documents to obtain banking and other services. In addition, by using the FVS some private sector organisations that may otherwise retain copies of identity documents as a record of their identity checks may not need to do so. Rather they can retain a transaction record as evidence of a successful FVS check. This will help minimise the risk of loss or theft of identification information from private sector organisations. Whilst there may also be service delivery benefits for the private sector, this is a secondary benefit and not the primary objective.

70. One submission refers to the statement in paragraph 145 of the EM that private sector users of the FVS will only receive a 'match or no match' response when using the FVS, and will not receive any facial image or biographic information. The submission notes that this feature is not in the Bill.[24] As noted in paragraph 145 of the EM, this feature will be implemented in access policies and data sharing agreements supporting the implementation of the Bill.

71. One submission appears to suggest that clause 17(1) of the Bill will permit private sector entities to collect 'sensitive information' (as defined in the Privacy Act).[25] This would be an incorrect interpretation of clause 17 of the Bill. Clause 17 of the Bill refers specifically to the 'Department'. Clause 17 only permits collection of identification information by the Department with administrative responsibility for the legislation (Home Affairs), and only for the purposes set out in clause 17. All collection, use and disclosure of identification information through the services by private sector organisations must have the consent of the person, collected in accordance with the APPs.

*Protection of information held by the private sector*

72. Some submissions raise a concern about the provisions in Part 4 of the Bill prohibiting unauthorised disclosure or recording of protected information, and whether these provisions should apply to the private sector and local government users.[26]

73. These provisions only apply to 'entrusted persons', defined to mean employees of the Department, including secondees, and contractors of the Department working on the NDLFRS or the identity-matching services.[27]

74. As noted in the EM, the Bill does not encompass the unauthorised disclosure and recording of protected information by other entities, such as users of the identity-matching services.[28] This would be inconsistent with the purpose of the Bill which is to authorise the Department to operate the technical systems to facilitate the services, with appropriate safeguards, not to govern the use of the services by all other participating entities. Any unauthorised recording or disclosure of information by these entities will continue to be covered by the existing legislation that applies to those entities.

---

[24] Submission 8, Law Council of Australia, para 29.
[25] Submission 9, Joint Councils of Civil L berties, para 17.
[26] Submission 8, Law Council of Australia, para 26; Submission 9, Joint Councils of Civil Liberties, paras 16-17.
[27] Identity-matching Services Bill 2018, subclause 21(4).
[28] EM to Identity-matching Services Bill 2018, para 203.

75. In the case of private sector entities, the applicable legislation will include the Privacy Act. It should be noted that under sub-paragraph 7(3)(d)(i) of the Bill, a private sector organisation will only have access to verification services if it is subject to the Privacy Act. One submission correctly noted that not all private sector organisations are automatically covered by the Privacy Act.[29] One effect of clause 7(3)(d)(i) of the Bill is that private sector organisations that are not automatically subject to the Privacy Act, such as small businesses, will only be able to use the FVS if they opt-in to coverage under the Privacy Act.

76. In addition, private sector users will only receive a 'match or no match' response when using the FVS, as is the case with the existing DVS. In other words, the FVS will not provide private sector users with any additional identification information to that which they have already collected. On this basis, and noting that all private sector use will be based on the consent of the individual involved, it is unnecessary to apply the information protection provisions in the Bill to private sectors users.

77. Another submission raises concerns that private sector or local government users of the FVS may not have adequate information security and governance procedures.[30]

78. As noted above, private sector users will be subject to the Privacy Act, including the APPs. APP 11 requires APP entities to take reasonable steps to protect information. In relation to local government users of the FVS, these users will usually be subject to state or territory privacy legislation, which has comparable information protection provisions to APP 11. If the local government authority is in a jurisdiction that does not have privacy legislation, the authority will only have access to the FVS if it opts in to coverage under the Privacy Act or a comparable arrangement.[31] Including a requirement to protect information in the Bill would duplicate these existing information protection arrangements.

## Proportionality and scope of measures in the Bill

79. A number of submissions raise concerns that relate to the proportionality of measures in the Bill and whether the scope of the services is appropriate. Information about the proportionality of the measures in the Bill is provided in the Human Rights Compatibility Statement attached to the EM. This submission only addresses specific issues raised in other submissions to the inquiry.

80. Three submissions argue that law enforcement should only be able to use the face-matching services in serious cases.[32] This issue is addressed in the Department's first submission at paragraphs 74-82. Other proportionality issues raised in submissions are addressed below.

*Proportionality under international human rights jurisprudence*

81. A number of submissions refer to international human rights jurisprudence and argue that the measures in the Bill are not consistent with this jurisprudence.[33] The cases referenced by the submissions deal with the collection of biometric information directly from members of the public and the retention of that information by police for law enforcement purposes. As

[29] Submission 9, Joint Councils of Civil L berties, para 17.
[30] Submission 4, Office of the Victorian Information Commissioner, para 3.
[31] Identity-matching Services Bill 2018, paragraph 7(3)(d). Under the Privacy Act, a local government authority can only opt in to coverage under the Privacy Act with the agreement of the relevant state or territory government.
[32] Submission 1, Future Wise and the Australian Privacy Foundation, p. 7; submission 8, Law Council of Australia, para 13; Submission 11, Australian Human Rights Commission, paras 91-92.
[33] Submission 1, Future Wise and the Australian Privacy Foundation, p. 7; Submission 2, Australian Lawyers for Human Rights, para 5.6; Submission 11, Australian Human Rights Commission, paras 44-46.

discussed above, the Bill does not seek to govern the collection of identification information, including biometrics, from individuals, nor the handling of identification information by agencies other than the Department of Home Affairs (as the operator of the systems authorised by the Bill).

82. The authorisations provided by the Bill simply enable the Department to make available tools to enable agencies to more securely share and match information. The key principle on which the services operate is that all participating agencies must have their own legal basis to collect, use and disclose the information they share through the services. This also applies to their collection of the primary biometric information from an individual (such as the collection of CCTV footage or passport photos), and their retention of that information for use through the services or otherwise. The Bill does not seek to expand police powers in relation to collection or retention of biometrics, nor authorise agencies other than the Department to use or share information where it is not otherwise authorised under other legislation.

*Whether the Bill should prohibit 'blanket surveillance'*

83. Some submissions raise concerns about the whether the Bill might authorise 'blanket surveillance' or 'real-time monitoring' of persons in public places.[34] The submissions argue that the Bill should specifically prohibit 'many-to-many' face matching through the services.[35]

84. The essence of the argument made in some of these submissions is that agencies may potentially use the FIS in relation to public gatherings or public places to monitor and identify members of the public *en masse*. However, any such use of the FIS would rely on the requesting agency and the data-holding agency having a legal basis to collect, use and disclose the identification information of individuals in that context, and would need to fall within one of the identity and community protection activities for use of the FIS listed in subsections 6(2) to (6) of the Bill. These restrictions, as well as practical impediments described in the Department's first submission, make it infeasible that the FIS would be used for this purpose in practice. More information about this issue is in paragraphs 64-67 of the Department's first submission.

*Whether the services can be used to determine a person's location*

85. One submission notes that the face-matching services could potentially be used to determine where a person has been at a given time.[36]

86. It is correct that use of the FIS, combined with other tools used by agencies to ascertain the identity of an individual, could assist an agency to determine that a person had been in a particular place at a particular time. However, agencies that will use the FIS already conduct identity-resolution activities that could reveal the same information. Indeed, many of the functions of national security and law enforcement agencies rely on their ability to place a particular person in a particular place at a particular time. Access to the FIS itself does not enable this – but rather it is the powers that agencies have under other legislation to collect personal information, including photographs, in the field and share this information for the purpose of identifying the individual.

[34] Submission 1, Future Wise and Australian Privacy Foundation, pp. 9-10; Submission 5, Civil L berties Australia, p. 2; Submission 11, Australian Human Rights Commission, paras 12(b), 91. .
[35] Submission 3, Queensland Office of the Information Commissioner, p. 3.
[36] Submission 4, Office of the Victorian Information Commissioner, para 2.

87. Although the FIS may facilitate this information-sharing, the issue of whether law enforcement and national security agencies should be able to determine where an individual has been would more appropriately considered in the context of those agencies' legal authorities to collect and share information, rather than this Bill.

*Whether use for prevention or promotion is legitimate*

88. Some submissions argue that use of the face-matching services for 'prevention' of offences or 'promotion' of security or safety (i.e. circumstances where a criminal offence or other event of concern has not yet occurred) would not be legitimate.[37]

89. The prevention of offences is recognised in Australian privacy law as a legitimate aspect of law enforcement. APP 3.4(d) permits the collection of sensitive information for 'enforcement related activities'. Similarly, APP 6.3 permits the use or disclosure of personal information for 'enforcement related activities'. The definition of 'enforcement related activities' in section 6(1) of the Privacy Act includes the 'prevention' of criminal offences.

90. The Bill includes the term 'promotion' in the definition of 'protective security', 'community safety' and 'road safety' activities. This is because some instances where the services may need to be used for those activities may not be able to be more specifically tied to a particular offence or instance of non-compliance. For example, in many community safety environments, a person may be reasonably believed to pose a threat to the community even if the specific nature of the threat or offence that they may commit is less clear. Similarly, an agency may have a need to verify the identity of a person in protective security context where a person is acting suspiciously in the near vicinity of a government facility. Or a road agency may seek to use the services to routinely check that driver licence applicants do not already hold a licence in another name, without having to have a suspicion that the particular applicant may be engaged in identity fraud for example.

91. This language is consistent with the IGA and provides an appropriate degree of flexibility to capture a range of activities that support the objectives of the Bill.

*Whether more information than necessary will be collected*

92. Some submissions argue that the Bill may enable more information than is necessary to be collected via the NDLFRS and identity-matching services.[38]

93. The Bill only authorises the Department to collect identification information for the purposes specified in clause 17. This is limited to collection for the purpose of maintaining and operating the NDLFRS, providing an identity-matching service, and other related purposes. Clause 5 of the Bill defines the scope of the identification information covered by the authorisation. The definition contains specific types of information that can be collected, and excludes other types. This ensures that the authorisation only covers those types of information contained in government identification documents and relevant to identity verification and identification for the activities permitted by the Bill.

[37] Submission 2, Australian Lawyers for Human Rights, para 5.4; Submission 11, Australian Human Rights Commission, para 77(a).
[38] Submission 1, Future Wise and the Australian Privacy Foundation, p. 7; Submission 8, Law Council of Australia, para 15; Submission 9, Joint Councils for Civil Liberties, para 37.

94. One submission raises a concern that health information might be used in the future in the identity-matching services.[39] However, subclause 5(2) of the Bill prevents the inclusion of health information, as defined under the Privacy Act.

*Retention of information obtained through the services*

95. Similarly, some submissions raise concerns at the length of time that data collected through the services may be retained. Two submissions recommend that data only be retained for the minimum period necessary.[40]

96. The Department supports this principle, noting that retention of data is already governed by a range of Commonwealth, state and territory legislation. The Face Matching Services Participation Agreement will provide that agencies that receive identification information through the face-matching services must only retain it for the minimum period of time that is necessary to fulfil the purpose for which it was obtained and comply with relevant laws that apply to the agency. After that period, the agency will be required to destroy the information.

*Whether alternative methods can be used*

97. One submission argues that methods other than facial recognition should be used to achieve the purposes of the Bill.[41]

98. The face-matching services facilitated by the Bill have been developed to address gaps in existing identification and identity verification activities.

99. The DVS is currently used by around one hundred government entities and seven hundred businesses, including all major finance and telecommunications companies, with more than 30 million DVS transactions processed in 2017.

100. Whilst expanding use of the DVS has made it harder for criminals to use fictitious identities, it is also creating incentives for them to use documents in stolen identities that have genuine biographic details (which will pass a DVS check) combined with a fraudulent photo. The biographic-based DVS cannot detect these fraudulent identities, creating a need for a different solution to tackle the growing use and sophistication of these stolen identities.

101. Despite widespread use of the DVS, and a range of other ad-hoc information-sharing arrangements between particular agencies for identity verification and identification, identity crime in Australia continues to have a significant impact.[42] The face-matching services have been designed to help address this issue within a framework of appropriate safeguards.

*Definition of 'identification information'*

102. One submission notes that clause 5 the Bill has a definition of 'identification information' that is different to the definition of 'personal information' in the Privacy Act, and queries whether this is intentional.[43] The submission argues that these differences may result in legal complexity

[39] Submission 5, Civil L berties Australia, p. 3.
[40] Submission 9, Joint Councils for Civil Liberties, recommendation 8(ii); Submission 13, Australian Human Rights Commission, recommendation 6.
[41] Submission 1, Future Wise and the Australian Privacy Foundation, pp. 8-9.
[42] See for example, *Identity Crime and Misuse in Australia Report 2016*, available at https://www.homeaffairs.gov.au/about/crime/identity-security/id-crime-australia.
[43] Submission 8.1, Law Council of Australia supplementary submission, para 5.

and a departure from existing standards for the protection of personal and sensitive information in the Privacy Act.

103. An explanation of the purpose of the definition of 'identification information', and the reason for its departure from the Privacy Act definitions, is set out in paragraphs 23-24, 43 and 62 of the EM. In summary, the definition is intentionally different from definitions in the Privacy Act, and is consistent with existing practice in the *Criminal Code Act 1995* (Criminal Code). Section 370.1 of the Criminal Code contains a separate definition of 'identification information' in the context of defining identity fraud offences.

104. The rationale for including a more limited definition of identification information, rather than aligning with definitions in the Privacy Act, is to restrict the types of information that the Department will be authorised to collect, use and disclose under the Bill. The types of information required for the services include some information that is 'sensitive information' under the Privacy Act, such as facial images and biometric templates. If the Bill aligned with Privacy Act definitions it would need to capture all 'sensitive information' under the Privacy Act, which would broaden the range of information to which the Bill's authorisations apply. As most of the information defined as 'sensitive information' in the Privacy Act is not necessary for the purposes of the identity-matching services, the more conservative approach of a standalone definition restricted to the necessary information has been taken.

105. The submission in question also notes that information about deceased people is captured by the definition of identification information. In practice, this type of information will not always be able to be separated from information about living people in the databases to which the services will connect. This information may also be necessary for some of the activities for which the identity-matching services may be used, including preventing and detecting identity fraud (for example, use of a deceased person's identity) and identifying a person who has died.

106. The collection, use and disclosure of all identification information by the Department under the Bill will also be covered by the information protection provisions in Part 4.

*Whether identification information can be used for profiling*

107. Some submissions argue that the definition of identification information in clause 5 of the Bill could allow the face-matching services to be use for racial or ethnic profiling, because this information may be inferred from information that is permitted to be collected.[44]

108. The Bill does not provide any authority for agencies to undertake these activities. The Bill does not authorise other agencies to collect, use or disclose identification information through the services. These agencies must have their own legal basis to do so, and remain subject to existing privacy protections and other controls that apply to their handling of that information.

109. As discussed above, the types of information that the Bill authorises the Department to collect, use and disclose are limited to those necessary to operate the services. As far as it is practicable to do so, the Bill (Subclause 5(2)) excludes the use of racial, ethnic or religious information, although there is an exception (Subclause 5(3)) which recognises that in some

[44] Submission 8, Law Council of Australia, para 14; Submission 9, Joint Councils of Civil Liberties, rec 3(i).

cases this information may be inferred from other information such as a person's name or facial image.

*Use of information for other purposes by the Department*

110. One submission suggests that the Department could use the interoperability hub to 'collect and aggregate data' and use that information for law enforcement or intelligence-gathering functions.[45]

111. However, as noted in paragraphs 170-173 of the EM, the interoperability hub does not store or collect information, it only relays electronic information. In addition, the Bill does not authorise the Department to collect, use and disclose identification information for purposes other than those set out in subclause 17(2), including maintaining and operating the NDLFRS, providing an identity-matching service, and other purposes related to the development and provision of the identity-matching services.

*Reliability of face-matching services*

112. A number of submissions question whether results obtained from using the face-matching services would be accurate.[46] There was concern that the face-matching services may sometimes provide false positive or false negative results.

113. In the case of the FVS, all queries will require some biographic information and in many cases information about the particular identification document which the user is seeking to match against (for example, a driver licence number). The system will then locate the corresponding record before conducting a biometric facial comparison within the system (if a photograph is included in the query) or returning a photograph for manual comparison. Limiting the functionality of the FVS to 'one-to-one' matching, using biographic information and/or a document number to identify a person's corresponding record, helps to minimises the risk of false matches. In addition, as is the case with the DVS, a match using the FVS should not be relied upon by a user as the sole basis for making an identity resolution decision.

114. Similarly, the one-to-many matching provided by the FIS will not rely on a completely automated process to identify a person. To reduce the possibility of false matches, results of FIS queries will need to be reviewed by a human operator to help determine the identity of the search subject. Under clause 9.9(d) of the IGA, the Face Matching Services Participation Agreement will require participating agencies to provide appropriate training to personnel using the services. This will include more stringent facial recognition training requirements for FIS users. This will ensure that users undertaking identity resolution activities are appropriately skilled to make identity decisions.

115. No identity-matching system is 100% accurate, which is why under the IGA, the identity-matching services are a non-evidentiary system. The results of the identity-matching services are not designed to be used as the sole basis for ascertaining an individual's identity for evidentiary purposes, and the agency using the services remains responsible for identity resolution. [47]

---

[45] Submission 1, Future Wise and Australian Privacy Foundation, para 7, p. 11.
[46] Submission 1, Future Wise and Australian Privacy Foundation, p. 8; Submission 8, Law Council of Australia, para 16; Submission 9, Joint Councils of Civil Liberties, para 36; Submission 11, Australian Human Rights Commissioner, paras 22-24.
[47] IGA, para 2.1(e) and (f).

116. One submission argues that the non-evidentiary nature of the identity-matching services should be set out in the Bill, to embed this core intent of the regime into law.[48]

117. However, as noted elsewhere in the submission, the Bill is not intended to govern other agencies' use of information obtained through the identity-matching services. This is already governed by a range of other legislation (including laws relating to the handling of evidence and criminal investigation procedures, privacy legislation and agency-specific legislation), which also govern agencies use of biometric information through other systems and processes that are outside the scope of the Bill. It would be impractical to attempt to cover such matters of evidence law in the Bill, which could result in inconsistent legislative regimes governing the use of biometric matching results for evidentiary purposes.

118. The Department recognises that there is a need for arrangements to assist persons who may be the subject of incorrect matching results. The Face Matching Services Participation Agreement and the NDLFRS Data Hosting Agreement established pursuant to the IGA will establish these arrangements, and the Department will make information available on a public website to assist individuals to raise these issues with the appropriate authorities.

*Whether a warrant should be required to use the FIS*

119. Two of the submissions argue that a warrant should be required for use of the identity-matching services, in particular for the FIS based on its increased privacy implications.[49] The Department responds to this issue in paragraphs 83-91 of its first submission, and provides the following further information in addition to that response.

120. The Department recognises that the privacy implications associated with the FIS are greater than those of the other identity-matching services. This is why the FIS is subject to greater privacy protections under the Bill and under supporting agreements and policies.

121. However, as noted in the Department's first submission, the Department does not agree that the Bill should require agencies to obtain a warrant to use the FIS.

122. The Attorney-General's Department's (AGD) *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers of 2011* (the Commonwealth Offences Guide) describes the circumstances when it would be appropriate to require agencies to obtain a warrant. The circumstances under the Commonwealth Offences Guide are:

- Where there is entry to premises without consent;[50]
- Where it is required to use reasonable force against things or persons in the execution of a warrant;[51]
- Where there is seizure of items;[52]
- Where there is a monitoring regime involving the above matters.[53]

123. Some Commonwealth legislation also requires a law enforcement agency to obtain a warrant in some circumstances in the investigation of offences. One example is the requirement under

[48] Submission 3, Office of the Queensland Information Commissioner, p. 3.
[49] Submission 10, Queensland Council for Civil Liberties, pp. 1-2; Submission 11, Australian Human Rights Commission, para 92.
[50] AGD, Commonwealth Offences Guide, para 8.1, p. 76.
[51] AGD, Commonwealth Offences Guide, para 8.3.4, p. 80.
[52] AGD, Commonwealth Offences Guide, para 8.5.1, p. 82.
[53] AGD, Commonwealth Offences Guide, para 8.7, p. 87.

the *Telecommunications (Interception and Access) Act 1979* for agencies to obtain a warrant to intercept a person's telephone conversations or obtain their stored communications such as emails. Another example is the requirement under the *Surveillance Devices Act 2004* for agencies to obtain a warrant to use a surveillance device in private premises. Under both of these types of warrants, the purpose is for the law enforcement agency to obtain new evidence consisting of the content of a person's private communications or actions in connection with the possible commission of an offence.

124. None of the circumstances referred to above apply in relation to use of the FIS. In using the FIS, the agency will submit a probe image of a person that it has already obtained lawfully. Use of the FIS does not involve entry into private premises, use of force, the seizure of items, the obtaining of private communications or the surveillance of a person. The Bill facilitates the sharing of information between agencies, but relies on agencies having a separate legal basis for that information-sharing. Police already share this information subject to their existing legal authority and in most cases, without a warrant. It is not appropriate for the Bill to apply an additional requirement on use of the services that does not already apply to other comparable electronic or manual means used by agencies to share information or identify a person.

## Rule-making powers in the Bill

125. A number of submissions raise concerns about the rule-making powers in the Bill. The Bill provides for the Minister to make rules prescribing:

- new types of identification information (paragraph 5(1)(n))
- new identity-matching services (paragraph 7(1)(f))
- an authority that can access the FIS, where the authority performs functions previously performed by a state or territory law enforcement or anti-corruption agency listed in paragraphs 8(2)(g) to (p) of the Bill (paragraph 8(2)(q)).

*Whether there should be a rule-making power*

126. Some submissions argue that the above rule-making powers in the Bill should not be present, and that these matters should only be governed directly in the Act.[54] In relation to this issue, the Department refers the Committee to paragraphs 34-48 of its first submission.

127. The submissions assert that use of a rule-making power means there would not be any parliamentary oversight.[55] This is not correct. Clause 30 of the Bill specifically provides that rules made under the Bill will be legislative instruments for the purpose of the *Legislation Act 2003* (the Legislation Act). Under sections 38 and 39 of the Legislation Act, all legislative instruments and their explanatory statements must be tabled in both Houses of the Parliament within 6 sitting days of the date of registration of the instrument on the Federal Register of Legislation. Once tabled, the rules will be able to be scrutinised by Parliament, including consideration by the Senate Standing Committee on Regulations and Ordinances.

128. Subclauses 30(3) and (4) of the Bill further provide that rules made under the Bill will be subject to disallowance and sunsetting, even though they would otherwise be exempt from these requirements under a general exemption in the Legislation Act for instruments that

[54] Submission 8, Law Council of Australia, paras 19-23; Submission 9, Joint Councils of Civil L berties, paras 11-14; Submission 11, Australian Human Rights Commission, paras 11, 12(d), 119-127.
[55] Submission 8, Law Council of Australia, para 20; Submission 9, Joint Councils of Civil Liberties, para 12.

facilitate the operation of an intergovernmental scheme involving the Commonwealth and one or more States.

*Rules versus regulations in the Bill*

129. Some submissions argue that the rule-making powers under the Bill should in fact be regulation-making powers. The submissions argue that regulations are subject to a higher level of executive scrutiny than other delegated legislation.[56]

130. The use of rules rather than regulations is consistent with the Office of Parliamentary Counsel's Drafting Direction No. 3.8 - Subordinate Legislation.[57] Paragraph 2 of that Drafting Direction states that:

> "OPC's starting point is that subordinate instruments should be made in the form of legislative instruments (as distinct from regulations) unless there is good reason not to do so".

131. Consistent with paragraph 16 of the Drafting Direction, the approach of including new identification information or identity-matching services in rules rather than regulations has a number of advantages including:

- it facilitates the use of a single type of legislative instrument when needed for the Act, thereby reducing the complexity that would otherwise exist if different matters were to be prescribed across more than one type of instrument
- it enables the number and content of legislative instruments made under the Act to be rationalised
- it simplifies the language and structure of the provisions in the Bill that provide the authority for the legislative instruments, and
- it shortens the Bill.

132. Due to these advantages, paragraph 17 of the Drafting Direction states that drafters should adopt this approach where appropriate with new Acts.

133. The Drafting Direction states that matters such as offence or civil penalty provisions, powers of arrest, detention, entry, search or seizure, the imposition of a tax, appropriations, and amendments to the text of an Act should be included in regulations unless there is a strong justification for prescribing those provisions in another type of legislative instrument. The Bill does not enable rules to include any of these types of provisions, and subclause 30(2) of the Bill specifically prohibits this for the avoidance of doubt.

## Security and data protection issues

134. A number of submissions raise concerns relating to the security of information that is collected, used or disclosed in the NDLFRS and the identity-matching services.[58] Similarly, a number of submissions raise concerns relating to possible data breaches or misuse of information.[59]

---

[56] Submission 3, Queensland Office of the Information Commissioner, p. 4; Submission 8, Law Council of Australia, para 23.
[57] OPC, http://www.opc.gov.au/about/draft_directions.htm.
[58] Submission 2, Australian Lawyers for Human Rights, paras 5.8-11;
[59] Submission 4, Office of the Victorian Information Commissioner, para 7; Submission 8, Law Council of Australia, paras 17-18;

135. Entities participating in the identity-matching services must continue to comply with privacy protections that apply to them, including the APPs where applicable. APP 11 requires entities to take such steps as are reasonable in the circumstances to protect personal information that they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. Where a state has privacy legislation, its agencies will be subject to the state's comparable privacy protections. Where the there is no privacy legislation in a state, under the Face Matching Services Participation Agreement, user agencies in those states will be required to comply with the APPs in their use of the services.

136. The development and operation of the NDLFRS and the inoperability hub by the Department will adopt best practice security and access arrangements. The systems will comply with the requirements of:

- the Australian Government Protective Security Manual, which provides guidelines and minimum standards in relation to protective security for Australian Government agencies and officers, and
- the Australian Government Information Security Manual, which sets out the standards that govern the security of government ICT systems.

137. The systems will also be subjected to independent penetration and vulnerability tests, an independent security review by the ASD and the Information Security Registered Assessors Program (IRAP) certification process, which is the best-practice Commonwealth information security assessment.

138. Access to the identity-matching services will be restricted to individuals that have been authorised by the participating agencies. Users will only be provided with access to the specific functions they have been authorised to perform. Most users will only be given access to the FVS function, and access to the FIS will be much more limited. For example, under the Face Matching Services Participation Agreement, FIS users will be required to have appropriate training in facial recognition, and must be monitored by a supervising officer when using the services.

139. Protection of information at participating agency-level will rely on existing data security controls that those agencies already apply when handling personal information. Within the framework of the Face Matching Services Participation Agreement, data-holding agencies will be able to stipulate any additional measures that they require to support the secure exchange of images. Regular audits will help ensure that these protections are functioning appropriately.

140. More generally, the identity-matching services will improve the security and accountability of information-sharing between participating agencies. Much information-sharing currently relies on ad-hoc or manual transmission of information, and can be difficult to audit or assess from a security perspective. By contract, the interoperability hub and NDLFRS will provide secure tools for information-sharing, with audit data captured on each transaction. By replacing a range of information-sharing practices with a single system subject to robust oversight, auditing and accountability requirements under the Bill, the IGA and associated arrangements, the services can increase the overall security and accountability of information-sharing between agencies.

141. As noted earlier in the submission, management of data breaches is governed by the new data breach notification provisions in Part IIIC of the Privacy Act. These provisions will apply to the information held or processed in the NDLFRS and the identity-matching services. In

addition, the identity-matching services will reduce the impact of data breaches on individuals and the community by helping to prevent the use of stolen identities obtained through data breaches. These stolen identities are often used by criminals for a range of purposes, exacerbating the impact of the identity breach for individuals. The identity-matching services will help to detect the use of these stolen identities, preventing further compromise of an individual's identity.

# Concluding remarks

142. The identity matching services enabled by the Bill will help to strengthen the integrity and security of Australia's identity infrastructure—the identity management systems of government agencies that issue Australia's core identity documents such as driver licences and passports. These systems play an important role in preventing identity crime, which is one of the most common and costly crimes in Australia that affects around 1 in 20 Australians every year with an estimated annual cost of over $2.2 billion[60], and is also a key enabler of serious and organised crime.

143. The Bill provides the Department with the authorisation it requires, subject to appropriate safeguards, to operate the technical systems that will facilitate information-sharing via the identity-matching services in a more efficient, secure and accountable way than many existing processes. It does not authorise any agency other than the Department to collect, use or disclosure identification information via the services. The Bill does not seek to expand the legal authorisation that other agencies have to share identification information through the services or otherwise.

144. The Department supports the need for robust privacy, transparency and accountability safeguards in relation to the provision and use of the identity-matching services. The Bill contains a range of safeguards to protect against misuse of this information. These protections are supported by a further layer of protections under the IGA and the policy and administrative arrangements that support the operation of the services, together with further protections that will apply through the application of the Privacy Act (including information security, information quality, information governance requirements, and the Notifiable Data Breaches scheme) and existing oversight by a range of Commonwealth, state and territory bodies.

[60] *Identity Crime and Misuse in Australia 2016* report, available at https://www.homeaffairs.gov.au/about/crime/identity-security/id-crime-australia.