Australian Government
Department of Home Affairs

April 2018

Parliamentary Joint Committee on Intelligence and Security

Department of Home Affairs Submission

Inquiry into the Identity-matching Services Bill 2018

Table of Contents

Introduction **3**

Overview of submission 3

Purpose and context of the Bill **4**

Purpose and background 4

Legislative context 5

Technical systems 6

Policy and administrative arrangements 6

Oversight arrangements 7

Proposed government amendments 7

Issues previously raised by the Committee **9**

Other issues **11**

Private sector access to the face-matching services 11

Access by agencies in South Australia and Western Australia 13

Whether the IMS Bill allows 'blanket surveillance' 13

Whether the statutory review provisions should be strengthened 13

Whether the Bill should specify the types of criminal offences for which the services can be used to identify people 14

Whether police should obtain a warrant before using the identity-matching services 15

Concluding remarks **17**

Introduction

1. The Department of Home Affairs welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence and Security as part of the Committee's inquiry into the Identity-matching Services Bill 2018 (the Bill).

Overview of submission

2. This submission provides an overview of the purpose of the Bill and the context within which it has been developed, including the other agreements and policy documents that, together with the Bill, govern the delivery and use of the identity-matching services.

3. In doing so, the submission outlines proposed amendments to the Bill which the Government intends to move to address recommendations made by the Senate Standing Committee on the Scrutiny of Bills in its *Scrutiny Digest No. 2 of 2018*.

4. The submission also addresses issues relating to the collection of biometric information raised by the Committee in its *Advisory Report on the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*.[1]

5. The submission then addresses other issues identified with the Bill in the context of a Queensland parliamentary inquiry into related legislation, the Police and Other Legislation (Identity and Biometric Capability) Amendment Bill 2018 (Qld), which enables that state's participation in the identity-matching services.

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

[1] Available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Counter-Terrorism_Legislation_Amendment_Foreign_Fighters_Bill_2014/Report1.

Purpose and context of the Bill

Purpose and background

7. The main purpose of the Identity-matching Services Bill 2018 is to authorise the Department of Home Affairs (the Department) to collect, use and disclose identification information in order to operate the technical systems that support the provision of identity-matching services, pursuant to the *Intergovernmental Agreement on Identity Matching Services* (the IGA)[2] agreed by the Council of Australian Governments on 5 October 2017.

8. These services provide the ability to use facial images and related identification information to: verify a person's claimed identity (for example, the Face Verification Service); and identify an unknown person or a person holding multiple fraudulent identities (for example, the Face Identification Service).

9. The sources of information available through the services include: visa and citizenship images held by the Department; passport images held by the Department of Foreign Affairs and Trade; and driver licence images held in a system hosted by the Department on behalf of the states and territories.

10. The identity-matching services established 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.

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

12. Identity crime is also a key enabler of serious and organised crime, including terrorism. Australians previously convicted of terrorism related offences are known to have used fake identities to purchase items such as ammunition, chemicals that can be used to manufacture explosives, and mobile phones to communicate anonymously to evade detection. An operation by the joint Australian Federal Police and New South Wales Police Identity Security Strike Team found that the fraudulent identities seized from just one criminal syndicate were linked to 29 high profile criminals linked to historic or ongoing illicit drug investigations, more than $7 million in losses associated with fraud against individuals and financial institutions, and more than $50 million in funds that were laundered offshore and were likely to be proceeds of crime.

13. The services will also assist with a range of other national security, law enforcement, community safety, and identity verification activities, including: the identification of unknown suspects in counter-terrorism or law enforcement operations; the provision of more secure and

[2] Available at https://www.coag.gov.au/about-coag/agreements/intergovernmental-agreement-identity-matching-services.

accessible government and private sector services to people using legitimate identification documents or whose documents are lost or damaged; and improving road safety through the detection and prosecution of traffic offences.

14. The Bill will form part of a broader legislative framework that governs the use of identification information by organisations participating in the identity-matching services. This legislative framework and associated independent and parliamentary oversight mechanisms is supported by a range of more detailed legal, policy and other administrative measures, contained in the IGA and other supporting data sharing agreements and policies. More information about the legislative context and supporting policy and administrative arrangements is provided below. Taken as a whole, this comprehensive range of privacy and security safeguards offers a continuum of control over the operation of the identity-matching services.

Legislative context

15. It is important to note that the Bill is not intended to govern the full operation and use of the identity-matching services. 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 provide.

16. In doing so, the Bill will become one part of a larger network of legislation that governs information-sharing between organisations participating in the identity-matching services. This includes the *Privacy Act 1988* (Cth), state and territory privacy legislation, and other legislation governing the specific functions and operations of agencies participating in the identity-matching services as providers or users of data.

17. The Bill does not seek to amend or replace this existing legislation, or to provide a blanket exemption to privacy legislation for organisations participating in the identity-matching services. Those agencies that make available data through the services, and those organisations seeking to access data through the services, will continue to be subject to legislative privacy protections and information-sharing restrictions that already apply to them. Agencies will need to have regard to their applicable legislative authorisations when participating in the services, including in relation to the organisations with which they can share information and the purposes for which they can do so.

18. In some cases new or amended legislation will need to be introduced to authorise or strengthen the legal basis for an organisation's participation in the identity-matching services. For example, the Australian Passports Amendment (Identity-matching Services) Bill 2018 is intended to strengthen the legislative basis for the Department of Foreign Affairs and Trade to make available passport information on an automated basis via the identity-matching services.

19. The Tasmanian Government recently amended its Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010, under the *Vehicle and Traffic Act 1999* (Tas), to strengthen its basis to share driver licence information for the purpose of participating in the identity-matching services. On 7 March 2018, the Queensland Parliament passed the Police and Other Legislation (Identity and Biometric Capability) Amendment Bill 2018, which strengthens the legal basis for the Queensland Government to do the same.

20. In other words, the Identity-matching Services Bill 2018 seeks to *enable* rather than to *authorise* the use of the services by various government agencies and (in more limited cases)

private sector organisations, which must have a basis to collect, use and disclose personal information under other legislation.

Technical systems

21. The technical systems that support the identity-matching services and which fall within the scope of the Bill are:[3]

    a. the interoperability hub, which supports the services by acting as a router to transmit requests for a face-matching service, and responses to those matching requests, between participating agencies; and

    b. the National Driver Licence Facial Recognition Solution (NDLFRS), which will comprise a federated database of state and territory licence information hosted by the Department on behalf of the states and territories, with an in-built facial recognition system to conduct face-matching against the database.

22. As the operator of these systems, the Department will not have access to the identification information contained in matching requests or responses that are routed through the interoperability hub, or to the facial images or other identification information stored in the NDLFRS. The Department will retain and have access to certain transaction data about matching requests and responses that is necessary for auditing and oversight purposes.

23. As set out in the explanatory memorandum, the Bill contains a range of privacy protections for the information handled by the Department in the course of developing and operating these systems. These include annual reporting on the provision of the services (clause 28), an offence for unauthorised disclosure of identification information by persons working on behalf of the Department (clause 21), and a statutory review (clause 29).

Policy and administrative arrangements

24. The legislative framework governing the use of the services provides a range of protections for the information that will be shared through the services. These legislative protections are just one aspect of the privacy safeguards surrounding the services. The IGA, as well as the legal, administrative and policy arrangements that the Department is putting in place to support its provision of the services, also contain further protections.

25. Under the IGA, these arrangements include additional privacy protections that participating agencies need to comply with before obtaining access to the services. These include:

    a. providing a statement of the legislative authority or basis on which the entity may obtain identity information through the face-matching services,

[3] Other systems which support the identity-matching services include the facial recognition databases operated by the Department of Home Affairs and Department of Foreign Affairs and Trade. Information held in these systems remains subject to other relevant legislation including the *Migration Act 1958*, *Australian Citizenship Act* 2007 and the *Passports Act 2005*.

b. being subject to a privacy impact assessment which includes consideration of the entity's use of the face-matching services (except where the entity's use is expressly exempt from relevant Commonwealth, state or territory privacy legislation),

c. entering into arrangements for the sharing of identity information with each data-holding agency it wishes to receive information from,

d. providing appropriate training to personnel involved in the use of face-matching services, and

e. conducting annual compliance audits in relation to the use of face-matching services.

26. These requirements will be set out in a common Face Matching Services Participation Agreement between all participating Commonwealth, state and territory agencies in order to provide a legally binding framework within which agencies will negotiate details of data sharing arrangements, so that these arrangements meet minimum privacy and security safeguards in order to support information sharing across jurisdictions.

27. These arrangements are being established and agreed between the Commonwealth and all states and territories. They are based on the principle that each state and territory retains control over decisions on how its data is shared.

28. The IGA provides for reviews to be undertaken at different points to provide mechanisms to ensure that the identity-matching services are being implemented and continue to operate as intended. These include a review of the Face Identification Service, 12 months after its commencement, and a review of the operation of the identity-matching services more broadly three years after the commencement of the IGA. Changes to this framework that may arise from these reviews will require broad national agreement, providing an additional level of control over any future expansion of the scope of the face-matching services.

Oversight arrangements

29. As indicated above, the Bill (clause 28) requires the Minister to report to Parliament annually on the operation of the services. This is an important transparency measure which will assist the Parliament with its oversight of the operation of the identity-matching services.

30. It is important to note that information sharing through the identity-matching services enabled by the Bill is part of the broader collection and use of personal information by agencies participating in the services. The use of the identity-matching services by those agencies, like those agencies' use of personal information more broadly, will be subject to a range of existing oversight mechanisms. These include the Information Commissioner and state and territory privacy commissioners, Commonwealth and state ombudsmen, and other oversight bodies such as the Inspector-General of Intelligence and Security, the Australian Commissioner for Law Enforcement Integrity and various state and territory equivalents.

Proposed government amendments

31. The Department would like to draw the Committee's attention to some minor amendments to the Bill that the Government will move in response to comments made by the Senate Standing Committee for the Scrutiny of Bills (the Scrutiny Committee) in its *Scrutiny Digest No. 2 of 2018*

tabled on 14 February 2018.[4] These proposed amendments may be relevant to the Committee's consideration of the Bill and any further amendments the Committee may recommend.

32. The Scrutiny Committee raised a number of issues focusing on the privacy implications of the Bill, as well as transparency and secrecy offence provisions. It made a number of suggestions for possible amendments to the Bill, and sought the Minister's response to these. In response, the Minister has agreed to seek to amend the Bill to:

    a. require the Minister to have regard to submissions made by the Human Rights Commissioner and the Information Commissioner when making rules to prescribe additional types of identification information or new identity-matching services,

    b. require the Minister to provide reasons explaining why the rules depart from that advice (if they do), and

    c. provide for annual reporting in relation to the number of instances in which an entrusted person discloses protected information to lessen or prevent a threat to life or health (under clause 23).

33. These amendments, if agreed by Parliament, would increase the transparency and accountability measures in the Bill. They will strengthen existing measures in the Bill that already provide for the Minister to consult with the Human Rights Commissioner and Information Commissioner when making rules, and to report annually on the provision of the identity-matching services, increasing the efficacy of those measures.

[4] Available at https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Scrutiny_of_Bills/Scrutiny_Digest.

Issues previously raised by the Committee

34. The Committee has previously considered issues relating to the collection and use of biometric information in its inquiry into the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 (the Foreign Fighters Bill).

35. The Foreign Fighters Bill amended the *Migration Act 1958* to provide for an authorised system (such as a SmartGate) to collect facial images from individuals entering and departing Australia, and use them to conduct biometric identification for immigration clearance purposes.

36. On introduction, the Foreign Fighters Bill also contained a further provision that would have enabled the relevant Minister to make regulations prescribing additional types of biometric data (such as fingerprints or iris scans) that could be collected and used by the authorised system for biometric identification in the future.

37. On 17 October 2014, the Committee issued its *Advisory Report on the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* (the Advisory Report). In its Advisory Report, the Committee expressed significant concerns about the regulation-making provision. In particular, the Committee was concerned that the addition of new categories of biometric data would not be subject to sufficient parliamentary approval or public comment if they were able to be added through regulations rather than a legislative amendment. The Committee recommended that the provision be removed from the Foreign Fighters Bill, and this recommendation was accepted by the Government.

38. In this context, the Department notes that the Identity-Matching Services Bill has a rule-making power at clause 5(1)(n) that would enable the Minister to prescribe additional types of identification information (which may include additional types of biometric data such as fingerprints or iris scans) that may be used in the identity-matching services.

39. However, there are three important features of the current Bill that distinguish it from the Foreign Fighters Bill and make it appropriate, in this case, to enable the Minister to prescribe new types of identification information in rules rather than through legislative amendment.

40. The first is that the Bill alone will not facilitate the collection from individuals of any new type of biometric data that may be prescribed in the rules. The Bill provides for the Department to collect, use and disclose identification information that is contained in an electronic communication to the interoperability hub or the NDLFRS. The Bill does not provide for the collection of biometric information directly from individuals.

41. Although the Bill provides for biometric information to be transmitted through the interoperability hub or the NDLFRS, the biometric information must have already been collected by a participating agency. Furthermore, the Bill does not authorise the sharing of identification information between other participating agencies – these agencies must have a basis to do so in other legislation. As such, the Bill provides a tool to enable data-sharing, but it is not intended to authorise participating agencies to collect identification information (including any newly prescribed biometric data) from individuals, or to share this information with other participating agencies through the identity-matching services.

42. In practice, this means that even where additional types of biometric data are prescribed in rules, agencies wishing to share such data through the services will also need to have a

separate legislative basis firstly to collect the biometric data from individuals, and then to share it with other agencies for one or more of the purposes for which the identity-matching services are available. An agency seeking to obtain that data through the services would also need to have a separate legal basis to do so.

43. Secondly, the rule-making powers in the Bill[5] contain a number of additional safeguards that will help to ensure rules are only made in appropriate circumstances and are subject to proper oversight. When making rules prescribing new types of identification information, clause 5(4)(a) provides that the Minister must be satisfied that the information being prescribed:

    a. can be used (alone or in conjunction with other information) to identify an individual; and

    b. is reasonably necessary to provide one or more identity-matching services; and

    c. assists one or more identity or community protection activities.

44. This will ensure that the Minister can only prescribe new types of identification information where that information is necessary and relevant to identification or identity verification for one or more of the purposes for which the identity-matching services are being provided.

45. In addition, the Minister will be required to consult the Human Rights Commissioner and the Privacy Commissioner when making any rules prescribing additional types of identification information (clause 5(4)(b)). As indicated above, the Government has also agreed to amend the Bill to strengthen this requirement to provide that the Minister must have regard to advice received from the commissioners, and must provide (most likely in an explanatory statement to the rules) reasons for any departure from the advice.

46. These provisions will ensure that privacy and other human rights considerations are a primary consideration in the development of any rules.

47. Thirdly, clauses 30(3) and (4) of the Bill specifically provide for the rules to be subject to disallowance by Parliament and sunsetting arrangements, even though they might otherwise have been exempted from these arrangements under ss44 and 54 of the *Legislation Act 2003*. These clauses have specifically been included to ensure appropriate oversight of rules made under the legislation, and that they are reviewed in a timely manner to ensure their ongoing relevance and currency.

48. By enabling the Minister to prescribe additional types of identification information in rules, subject to the safeguards discussed above, the Bill is designed to accommodate future changes in technology and data-collection practices. This is an appropriate approach given the facilitative nature of the Bill, which is intended to enable rather than authorise information sharing by agencies using the identity-matching services.

[5] The rule-making powers in the Bill are in clauses 5(1)(n), 7(1)(f) and 8(2)(q).

Other issues

49. The Queensland Parliament recently passed related legislation, the Police and Other Legislation (Identity and Biometric Capability) Amendment Bill 2018 (the Queensland Bill) to provide a legislative framework to facilitate Queensland's participation in the identity-matching services (including the face-matching services).

50. The Queensland Parliament's Legal Affairs and Community Safety Committee (the Queensland Committee) inquired into the Queensland Bill and invited submissions from a number of key stakeholders, including the Queensland Office of the Information Commissioner (Queensland OIC)[6]. The Queensland Privacy Commissioner, Mr Phillip Green, appeared before a hearing of the Queensland Committee.

51. Although the submissions largely focused on the provisions of the Queensland Bill, some also touched on the broader legislative framework for the face-matching services, including the Commonwealth Identity-matching Services Bill 2018. In anticipation that similar issues may be raised by stakeholders in submissions to the Committee's inquiry into the Commonwealth Bill, or otherwise considered by the Committee, the Department will address in this submission some of the concerns raised in submissions to the Queensland Committee's inquiry.

Private sector access to the face-matching services

52. The Queensland OIC and Privacy Commissioner raised concerns about private sector access to the face-matching services. In his appearance, Mr Green expressed concern that there may not be a specific mechanism in the legislation for controlling which privacy sector organisations would get access to the services. In the OIC submission, the OIC also noted that a privacy impact assessment has not yet been done in relation to potential private sector access.

53. Private sector organisations conduct a range of identity verification activities on a daily basis and are a key partner in combatting identity crime and other criminal activity such as money laundering and the financing of terrorism. Since 2014, private sector organisations have accessed the Government's Document Verification Service (DVS), a secure online service to help verify information on proof of identity documents. The service is currently used by more than seven hundred businesses, including all major finance and telecommunications companies. Private sector DVS users submitted around 15 million of the more than 30 million DVS transactions processed in 2017.

54. Expanding use of the DVS is making it harder for criminals to use fictitious identities, but is creating incentives for them to use documents in stolen identities. Providing the private sector with access to the Face Verification Service (FVS) will help prevent this from occurring, protecting the identities of innocent Australians and helping companies such as financial institutions and telecommunications providers to better meet their regulatory customer identification obligations that help to contribute to national security and law enforcement outcomes.

---

[6] Information about the Queensland inquiry, including copies of submissions, is available at http://www.parliament.qld.gov.au/work-of-committees/committees/LACSC/inquiries/current-inquiries/POLABILL2018.

55. Private sector access to the FVS would be on similar terms to the DVS, notably that they must collect the consent of individuals before seeking to match images through the service. Governance of the DVS involves robust contractual arrangements and a comprehensive programme of independent audits of users of the services which has resulted in suspension of access to the service for some entities for non-compliance with DVS terms and conditions.

56. With this in mind, private sector usage of the services is envisaged under clause 5.3 of the IGA. In order to fully implement the IGA, the Commonwealth Bill facilitates future use of the face-matching services by the private sector.

57. Clauses 7(2)-(4) and clause 10(2) of the Bill apply a range of privacy safeguards to private sector usage of the services. These include:

    - the private sector will only have access to verification services (not services for identifying unknown individuals)
    - verification of a person's identity must be reasonably necessary for the functions of the organisation (this includes organisations that are required or authorised by law to verify a person's identity)
    - the organisation must have a legal basis to use the service
    - the organisation must have the consent of the person whose identity is being checked
    - the organisation must be subject to the Commonwealth *Privacy Act 1988* (the Privacy Act)
    - the organisation must carry on activities in Australia or reside in Australia, and
    - private sector usage of the services will be reported on in the annual report to be tabled in Parliament (although the annual report does not require the publication of the names of specific private sector organisations to protect commercial confidentiality).

58. Subject to the passage of the Bill, the nature of private sector access remains a matter for Ministers at the Commonwealth and state and territory level to determine, guided by the IGA. Under clause 5.4 of the IGA, access to state or territory data for private sector users will also be subject to further safeguards, including:

    - the written agreement of the relevant state or territory minister
    - a privacy impact assessment covering the particular type of organisation seeking access
    - compliance with the Commercial Service Access Policy, and
    - an audit and compliance program.

59. In addition, private sector users will only get a 'match / no match' response, with no provision of biographic or photo information to the organisation.

60. These safeguards will ensure that private sector access to the face-matching services is appropriately limited and proportionate to their need to verify identity in the provision of services.

Access by agencies in South Australia and Western Australia

61. In his appearance before the Queensland Inquiry, the Queensland Privacy Commissioner raised a concern that government agencies in South Australia and Western Australia, states which do not have privacy legislation, would have access to the face-matching services.

62. Mr Green gave a theoretical example of a South Australian government official having unauthorised access to Queensland information. Mr Green stated that neither the Queensland Privacy Commissioner nor the Commonwealth Privacy Commissioner would have jurisdiction in such a case.

63. This issue will be addressed via the legally binding Face Matching Services Participation Agreement mentioned above. Under this Agreement, it is proposed that agencies in states and territories without privacy legislation (South Australia and Western Australia) will be required to comply with the Australian Privacy Principles under the Privacy Act in relation to their use of the face-matching services.

Whether the IMS Bill allows 'blanket surveillance'

64. In its submission to the Queensland Inquiry, the Queensland OIC expressed concern that the Commonwealth Bill did not 'explicitly protect against or prohibit the expansion of [the identity-matching services] to many-to-many, blanket surveillance techniques'. The Queensland Privacy Commissioner also expressed concerns about the risk of 'mass surveillance' in his appearance before the Queensland Committee.

65. All collection, use and disclosure of personal information through the face-matching services will be subject to relevant law, including the general privacy protections in the Australian Privacy Principles contained in the *Privacy Act 1988*. The purpose and effect of the Bill is to authorise the Department to deliver the services via the interoperability hub, and the operation of the National Driver Licence Facial Recognition Solution. The Bill does not authorise other agencies to undertake 'mass surveillance'. The Australian Privacy Principles will continue to operate to prohibit collection, use or disclosure of personal information that is not authorised by law.

66. The Bill will enable the Department to provide agencies with the tools to quickly and securely share and match data that they can lawfully collect, use and disclose to other agencies. Participating agencies need to have their own legal basis to collect information that they wish to use in a query or receive in response to a query, and to share it in the course of one or more of the identity and community protection activities, before they can use the services.

67. The Department also considers that 'mass' or indiscriminate use of the face-matching services would not be feasible in practice, given that the systems supporting the services are not designed to support this type of usage and that agencies would not have the resources, including personnel sufficiently trained in facial recognition, to devote to this kind of usage.

Whether the statutory review provisions should be strengthened

68. The Queensland OIC raised a concern in its submission to the Queensland Inquiry about whether the statutory review provision in clause 29 of the Commonwealth Bill should be strengthened. The Queensland OIC was concerned the only requirement in the Bill is for a

review to commence within five years of commencement and that the Bill does not specify the scope and content of that review.

69. The implementation of the face-matching services across all jurisdictions will be incremental over the next few years. A period of up to five years to commence a review of the services is appropriate to ensure that adequate information is available from each of the jurisdictions to ensure the review is thorough and comprehensive.

70. In addition, the statutory review period of five years is consistent with other Commonwealth legislation providing for statutory reviews. For example, section 251 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* provided for a review to be conducted within seven years.

71. The Commonwealth Bill does not specify the scope or content of the review. This is to ensure that conduct and content of the review is flexible to ensure that all relevant matters may be included without restriction. It is also intended to allow flexibility about the most appropriate arrangements for the review, taking into account government policy and practices at the time.

72. The Bill provides that the report on the review must be tabled in Parliament. This will ensure that the review is carried out to a high standard and covers all appropriate matters.

73. It is important to note that the statutory review is only one of a number of reviews of the face-matching services that will be implemented over the next few years. Under the IGA, the operation of the identity-matching services will also be subject to review every three years from commencement of the IGA (in October 2017). These reviews will be conducted under terms of reference determined by the National Identity Security Coordination Group, which is a senior management level group comprising representatives from lead agencies in the Commonwealth and each of the states and territories. These reviews will be provided to the Ministerial Council for Police and Emergency Management, providing accountability between the Commonwealth and the states and territories in relation to the provision and operation of the services.

Whether the Bill should specify the types of criminal offences for which the services can be used to identify people

74. The Face Identification Service (FIS) enables user agencies to identify an unknown person, or persons with multiple fraudulent identities. Under the IGA, use of the FIS is limited to certain permitted purposes, including law enforcement. The law enforcement purpose as it relates to the use of the FIS is defined in the IGA (clause 4.21 (b)) as 'the prevention, detection, investigation or prosecution of an offence under Commonwealth, state and/or territory laws carrying a maximum penalty of not less than three years' imprisonment)'.

75. In its submission to the Queensland Inquiry, the Queensland OIC noted that the Commonwealth Bill does not include detail on the types of offences for which the FIS can be used.

76. It is important to note that the Bill is part of a broader framework of legislative and policy controls over the operation of the identity-matching services (including face-matching services such as the FIS) which also comprises: other legislation governing the agencies participating in the services; the IGA and the Face Matching Services Participation Agreement within which agencies settle the details of their data sharing arrangements.

77. The 'identity and community protection activities' for which the identity-matching services may be provided are set out in clause 6 of the Bill, with the law enforcement activity in clause 6(3).

78. While the three-year 'offence threshold' has not been included in the Bill itself, it will apply in practice to the sharing of data between jurisdictions, through the application of the provisions in the IGA.

79. In doing so it is important to maintain a degree of flexibility to accommodate variations in criminal offences and penalties across jurisdictions. For example, some states have penalties of less than three years for serious offences such as assault. A blanket three year 'offence threshold' would render the FIS unable to be used by police investigating those offences in those jurisdictions. This is why the IGA (at clause 4.22) also provides for the FIS to be used by agencies *within the same jurisdiction* for law enforcement purposes in relation to offences with penalties of less than three years.

80. This flexibility will ensure that an arbitrary threshold requirement does not limit the ability of particular jurisdictions to use their own data (and possibly data from other jurisdictions with their agreement) for law enforcement purposes where they may have lower penalty for an offence that would meet the 'penalty threshold' in other jurisdictions.

81. The Department also notes that clause 4.25 of the IGA provides for a review of the operation of the law enforcement usage of the FIS twelve months after the FIS commences operation.

82. It is important to note that the Commonwealth Bill does not require any agency to provide its data for the identity-matching services, or to make its data available via the services for all of the identity and community protection activities. This is consistent with one of the key principles underpinning the IGA, that states and territories retain control over which organisations may their data and for what purposes.

Whether police should obtain a warrant before using the identity-matching services

83. It its submission to the Queensland Inquiry, the Queensland Council of Civil Liberties (QCCL) raised concerns about police accessing databases of identification information without first obtaining a warrant, unless the offence they are investigating relates to the purposes for which the data was collected (for example, accessing driver licence data to investigate traffic offences).

84. As the QCCL submission noted, the Commonwealth Bill does not contain a requirement that police or other agencies obtain a warrant before using the face-matching services. Part of the reason for this is because the Commonwealth Bill is not intended to regulate access to the services by other agencies.

85. However, the IGA also does not contain this requirement and the Department does not support a requirement for any law enforcement or other agency to be required to obtain a warrant before using the services. Such a requirement would have a significant impact on the ability of law enforcement or other agencies to use the services in the course of their activities.

86. The Department notes that the Bill is designed to facilitate access to information for certain purposes, by agencies that have a lawful basis to do so under other legislation. There are relatively few circumstances where law enforcement agencies would need a warrant to obtain

information needed to identify a person, or to verify a claimed identity. In addition, the governance arrangements for access to the services, particularly the FIS, have strict controls to ensure access is lawful and proportionate.

87. The face-matching services are designed to provide fast and automated access to identity verification and identification using facial images. One of the purposes of the services is to assist law enforcement and national security agencies to identify persons of interest in their investigations and other activities by providing them with better tools to share and match information than those currently available to them. One of the key benefits of this will be the increased speed with which these agencies can determine the identity of a person of interest, and take any steps necessary to protect the community from harm.

88. While it is not yet clear how often government agencies will use the services, it is likely that a requirement to obtain a warrant would effectively prevent government agencies from using the services, or obtaining the benefits of the services, in many cases.

89. Obtaining a warrant is a resource intensive process, both for the applicant agency and for the issuing authority hearing the application, which would presumably be members of the judiciary and members of the Administrative Appeals Tribunal. The time involved in preparing, reviewing and granting a warrant application to use services would:

    - significantly delay, and in some circumstances undermine, law enforcement and national security investigations
    - impede operational activity, including the prevention of criminal acts, and
    - divert resources from investigations.

90. The privacy benefits of requiring agencies to obtain a warrant would likely be significantly outweighed by the decreased ability of agencies to carry out their law enforcement and national security functions.

91. The Department considers that the privacy safeguards built into the Bill, as well as those contained in the IGA and administrative and policy arrangements supporting the services, are sufficient to ensure that the services are only used in appropriate circumstances and by appropriate authorities. Judicial oversight of each individual circumstance of potential use by a law enforcement agency would significantly limit the effectiveness of the services, and of the agency in performing its essential community protection functions.

Concluding remarks

92. The Department supports the need for robust privacy, transparency and accountability safeguards in relation to the provision and use of the face-matching services. The Bill has been designed to avoid a blanket authorisation for the use of the services by participating agencies, ensuring that information-sharing between two other agencies through the services will continue to be subject to existing privacy and other legislation.

93. The Bill contains a range of safeguards to protect against misuse of the information collected by the Department in the course of providing the services. These protections are supported by a further layer of protections under the IGA and the administrative and policy arrangements that support the operation of the services; all of which operates in the context of agencies existing oversight arrangements. Together, this legislative and administrative framework will ensure that participating agencies can access the tools they need to support their identification and identity verification activities whilst protecting the security and privacy of the information shared through the services.