July 2017

Privacy Impact Assessment for the Face Identification Service

Attorney-General's Department's Response

This is a response by the Attorney-General's Department (AGD) to the report of a Privacy Impact Assessment (PIA) on the use of the Face Identification Service (FIS) by specified agencies, finalised in March 2017.

AGD commissioned Information Integrity Solutions Pty Ltd (IIS) to conduct an independent PIA to evaluate any privacy impacts that may be associated with the use of the FIS by the Department of Immigration and Border Protection (DIBP), as a Data Holding Agency; and the Department of Foreign Affairs (DFAT) and the Australian Federal Police (AFP), as consumers of data (Requesting Agencies).

This response was prepared in consultation with DIBP, DFAT, AFP, the Inspector-General of Intelligence and Security and the Office of the Australian Information Commissioner.

The FIS is one of the services provided through the National Facial Biometric Matching Capability (the Capability), which is being developed and implemented by AGD. The FIS enables a facial image associated with an individual to be compared on a one-to-many basis against images held in government records to help determine the identity of that individual, or to detect instances where an individual holds multiple potentially fraudulent identities.

IIS has made nine recommendations on the design and governance of the FIS. AGD has accepted seven recommendations and accepted in principle the remaining two recommendations.

AGD acknowledges the privacy risks inherent in a system which shares personal information, and is committed to a privacy by design approach to manage those risks, and transparency in the use of the FIS. AGD will continue to commission independent PIAs into aspects of the Capability as part of this privacy by design approach.

This PIA builds on previous PIAs done in relation to the Capability, namely the 2015 PIA of the Interoperability Hub and the 2016 PIA of the Face Verification Service.

RECOMMENDATION	RESPONSE
1. Programme Advisory Committee to include Privacy Commissioner or representative IIS recommends that while the Programme Advisory Committee acts as the Face Identification Service Governing Body it should include the Privacy Commissioner, or the Commissioner's nominated representative. The Commissioner or nominated representative should have a role equivalent to that which the Commissioner would hold on the National Identity Security Coordination Group when it takes on the role of the Governing Body for the Capability.	**ACCEPT** AGD accepts that it would be appropriate for the Privacy Commissioner or nominated representative to be a member of the Programme Advisory Committee (PAC) or the National Identity Security Coordination Group (NISCG), whichever is the Governing Body. We have invited the Office of the Australian Information Commissioner (OAIC) to become an observer on the PAC. The draft Intergovernmental Agreement on Identity Matching Services provides that the NISCG will include representation, as an observer, from the OAIC.
2. Access Policy to ensure clear responsibility for privacy and for oversight of agency use of the Face Identification Service IIS recommends that the Attorney-General's Department and the Governing Body ensure that the Face Identification Service Access Policy or another appropriate, publicly available and binding governance document, set out clearly their respective privacy roles and responsibilities, in particular in relation to: • Overall privacy governance • The secretariat role to the Governing Body • Reviewing Interagency Data Sharing Arrangements to ensure consistency with the Access Policy • Reviewing annual audit and compliance reports to identify the need for compliance action or amendments to policy • Which entities are expected to take steps to address any compliance or audit issues.	**ACCEPT** The Access policy clearly sets out the respective privacy roles and responsibilities of AGD and the Governing Body, in accordance with this recommendation.
3. Monitoring national security use of Face Identification Service IIS recommends that the Governing Body ask the Inspector-General of Intelligence and Security, where it has relevant oversight responsibility, to give priority for a period to monitoring use of the Face Identification Service particularly with respect to the requirements of the Face Identification Service	**ACCEPT IN PRINCIPLE** AGD and the Inspector-General of Intelligence and Security (IGIS) agree in principle that the use of the FIS by the National Intelligence Community should be subject to oversight by the IGIS office. However, additional oversight responsibilities for the IGIS require additional resources and at this point it is unlikely the IGIS would be able to prioritise FIS over current inspections and

RECOMMENDATION	RESPONSE
Access Policy and to report on use to the extent consistent with national security obligations.	inquiries given its limited resources. If the IGIS is to oversight use of the FIS by National Intelligence Community agencies, the IGIS will require access to relevant audit reports, including details of the nature, number and purpose of searches conducted by each agency. The National Intelligence Community agencies will need to implement mechanisms to ensure only the required information is retained.
4. Interagency Data Sharing Arrangement to require adoption of privacy governance framework IIS recommends that the Attorney-General's Department amend the Interagency Data Sharing Arrangement template to include privacy governance and management standards, for example as per the Office of the Australian Privacy Commissioner privacy management framework, as well as security accreditation requirements.	**ACCEPT** Under the Participation Agreement, which all agencies will have to sign before they may use the FIS, Agencies will be required to develop and/or amend, as necessary, its privacy governance framework and management standards and reflect the management of the flow of information through the FMS. The Participation Agreement also contains clauses dealing with security accreditation requirements.
5. Holding and Requesting Agencies to have privacy policies and procedures that address use of one-to-many facial matching IIS recommends that the Australian Federal Police, Department of Immigration and Border Protection, and the Department of Foreign Affairs and Trade ensure their respective privacy policies, operating procedures and guidance materials be augmented where necessary to address the particular privacy risks associated with one-to-many facial matching and the agency's approach to managing associated privacy risks. In particular, agencies should ensure: • Their application forms, privacy policies and other privacy material provide appropriately detailed information about the use or disclosure of information for face matching activities • Their policies and procedures address the limitations or constraints of facial recognition technology and the associated privacy risks, including the risk of false positives, and the steps the agency will take to minimise the potential for harm to individuals.	**ACCEPT** The AFP, DIBP and DFAT will review their privacy policies, operating procedures, guidance materials and other relevant material to ensure that they address the privacy issues raised by one-to-many facial matching, in accordance with the recommendation.
6. Publication of information about Face Identification Service use	**ACCEPT**

RECOMMENDATION	RESPONSE
IIS recommends that the Attorney-General's Department or the Governing Body, in consultation with Data Holding Agencies and Requesting Agencies: • Publish annual reports on the usage of the Face Identification Service, by Holding Agency and Requesting Agency, with sufficient detail to enable an understanding of the volume of use and the purposes for which it is used • Publish Face Identification Service audits identifying any issues and the remediation planned. The documents should be published in full, or to the greatest extent possible in the event that an Agency is prevented from publishing them in full for security or other reasons.	AGD will publish annual reports on the usage of the FIS to enable a general understanding of the volume of use and the purposes for which it is used. AGD will include in these reports relevant information on the outcomes of FIS related audits, to the extent that it does not compromise operational security and agency methods.
7. Amendments to Face Identification Service Access Policy to be subject to a privacy impact assessment IIS recommends that the Governing Body commission an independent privacy impact assessment before making any substantive changes to the Access Policy (once finalised) with respect to expanding the purposes for which Requesting and Holding Agencies can share facial images.	**ACCEPT** AGD agrees that further PIAs should be undertaken on any substantive changes to the FIS Access Policy.
8. Additional auditing requirements where Face Identification Service is used for community safety IIS recommends that the Attorney-General's Department amend the Face Identification Service Access Policy to require that the proposed annual audits must examine community safety purpose requests taking into account the greater privacy risks. The aim should be to identify if, in addition to meeting requirements of the Access Policy, the use is likely to be consistent with community expectations about the use of face matching in such contexts as expressed, for example, by the qualifications currently included in the draft Access Policy or in relevant privacy regulator guidance or as identified following discussions with privacy regulators. IIS also recommends that detailed information about uses for community safety be published, for example by inclusion in reports such as are proposed in Recommendation 6.	**ACCEPT IN PRINCIPLE** The FIS Access Policy requires audits of Requesting Agencies to examine the queries relating to the permitted purpose of community safety, taking into account the greater privacy risks and whether authorisation was obtained for those circumstances that require authorisation. Agreements to share information between agencies participating in the FIS will require annual audit reports to examine the nature and number of searches identified as being for the 'community safety' purpose and whether they take into account the increased privacy risk of this purpose. As noted in relation to Recommendation 6, AGD agrees that there should be annual reporting on the usage of the FIS. AGD agrees that reporting should indicate the general purpose for which the service is being used, including where it is used for the community safety purpose.

RECOMMENDATION	RESPONSE
9. Extra protection for the handling of minors' images IIS supports AGD proposals to explore technical options to minimise the privacy and other risks that could arise where there are requests to match minor's images. It recommends that AGD and Requesting Agencies, in consultation with Data Holding Agencies, also review the specific privacy risks that might arise for minors where their images are matched and assess if additional protections are needed, for example, in the handling of images or in the applicable investigation standards.	**ACCEPT** AGD has implemented technical options to protect the interests of minors by imposing age restrictions on searches and requiring additional authorisation to search images of minors in most cases. AGD is open to considering further technical controls where this is technically feasible and warranted. The Access Policy requires agencies to review their internal business processes to ensure adequate safeguards and policies are in place to address any risks associated with matching the images of minors.