Australian Government
Attorney-General's Department

September 2016

Privacy Impact Assessment for the Face Verification Service

Attorney-General's Department Response

The Attorney-General's Department (AGD) commissioned Lockstep Consulting to conduct an independent Privacy Impact Assessment (PIA) on initial use of the Face Verification Service (FVS). The FVS is one of the services provided through the National Facial Biometric Matching Capability. The FVS helps agencies to verify a person's identity by matching their facial image (on a one-to-one basis) against one of their government records associated with an evidence of identity document.

This PIA builds on the preliminary PIA of the Interoperability Hub of the capability, conducted in 2015, to examine the use of the FVS by an initial set of Australian Government agencies. Specifically, this PIA covers use of the FVS by the Department of Foreign Affairs and Trade (DFAT) and the Australian Federal Police (AFP) to access citizenship and visa data held by the Department of Immigration and Border Protection (DIBP) through the three functions of the FVS:

1. *Retrieve* – returns a single facial image and corresponding biographic details in response to a text-based search
2. *Match* – involves a check against a particular record, identified by a unique identifier such as a document number, in order to return a single matching record (or in some cases a simple 'Yes/No' response) and
3. *Search* – involves a check of one or multiple records with matching biographic details, in order to return a single matching record.

The PIA comprises four reports which are structured as follows:

1. DFAT's use of DIBP's FVS Retrieve function for citizenship and visa data
2. AFP's use of DIBP's FVS Retrieve function for citizenship and visa data
3. DFAT's use of DIBP's FVS Match and Search functions for citizenship and visa data, and
4. AFP's use of DIBP's FVS Match and Search functions for citizenship and visa data.

Although AGD is not using the FVS, the PIA made some recommendations relevant to AGD in its role as the operator of the Interoperability Hub. Reports 1 and 2 contained no recommendations. Reports 3 and 4 each contained five recommendations, which were identical apart from the parties to which they related (i.e. AFP or DFAT). Of the five recommendations in Reports 3 and 4, four relate to AGD. The Department has accepted these recommendations.

AGD will continue to commission independent PIAs into aspects of the National Facial Biometric Matching Capability, as part of a privacy by design approach that the Department is taking to the implementation of this initiative.

RECOMMENDATION	RESPONSE
1. AGD should consider creating a privacy statement specific to the FVS hub, to address generally recognised privacy concerns around biometrics, and to explain to the public the major data protection properties of the NFBMC. Such a privacy statement could cover the NFBMC design philosophy, key procedural and technological data protection measures, and the high level rules, like DIBP and DFAT/AFP being required to enter into a bilateral data sharing agreement, and publish this PIA.	**ACCEPT** AGD will create a privacy statement for the Face Matching Services (FMS), covering the FVS and the Face Identification Service. This privacy statement will complement AGD's departmental privacy policy. The privacy statement will be made publicly available on AGD's website.
2. The FVS portal, at the time that a *Match* or *Search* is requested, should display a reminder to users of their obligations as officers of DFAT/AFP to treat all Personal Information in accordance with the Privacy Act and other relevant terms of their employment conditions.	**ACCEPT IN PART** AGD has designed the Hub Portal (through which DFAT/AFP users will access the FVS) to display welcome text on its home page. This text will remind users, each time they log on to the Portal, to treat all Personal Information in accordance with the Privacy Act and other relevant terms of their employment conditions. AGD considers that this approach should be sufficient to meet the intent of this recommendation and that it is not necessary for such a reminder to be displayed each time a Match or Search is requested. In addition, the Interagency Data Sharing Arrangement (IDSA) that DIBP enters into with each requesting agency includes undertakings that the agency's staff will abide by legislative provisions to protect DIBP identifying information.
3. Ensure that DFAT/AFP understands the limited event logging of the hub, and the need to cater for its own logging and auditing requirements. In particular, ensure that DFAT/AFP system designers understand that biometric algorithm and matching parameters are not retained by FVS and may not be made available by FVS if ever needed.	**ACCEPT** AGD has developed an IDSA template, which it has provided to DFAT/AFP and DIBP. The IDSA template specifies transaction data that the Hub makes available for a Requesting Agency, such as DFAT/AFP, to download for its audit purposes, as well as audit data that the Requesting Agency will need to generate for its own purposes, in order to fulfil record keeping requirements under the template IDSA. AGD has also developed Functional Specifications for the Retrieve, Match and Search Functions, each of which includes a list of audit data retained by the Hub. These

RECOMMENDATION	RESPONSE
	specifications indicate that biometric algorithms and matching parameters are not included in the audit data retained by the Hub. These specifications are available to current DFAT/AFP system designers and the system designers of Agencies who may use the FVS in the future.
4. AGD should consider adding advice to the IDSA guidance that requesting agencies (DFAT/AFP in this case) locally record details from time to time of the biometric algorithms used by the holding agency (DIBP here), in case future investigations of, for example, false matches, need to reference the algorithms and parameters applied in each usage of the FVS.	**ACCEPT** The IDSA template that AGD has developed includes a guidance note giving effect to this recommendation. In addition, the IDSA template requires the Requesting Agency to acknowledge its responsibility for assessing the impact of any changes to the Data Holding Agency's Threshold Specifications (thresholds for a biometric Match or No Match result) and its facial recognition and supporting systems on the Requesting Agency's use of the FVS. The IDSA template also requires the Requesting Agency to maintain records to facilitate its assessment of these impacts.
5. DFAT/AFP should retain its own records of all biometric matching parameters and other configuration information (algorithms, biometric product version numbers etc.) used by DIBP to produce each *Match* or *Search* result. Algorithm updates, especially changes to threshold parameters used for matching or searching, will change the performance of the processes from time-to-time, and these changes should be tracked by DFAT/AFP, so that in the event that a dispute arises, the precise conditions of past matches are not lost.	**ACCEPT IN PART** The biometric algorithms and matching parameters used by DIBP to support matching via the FVS are negotiated between DIBP and Requesting Agencies. DIBP will maintain a record of the algorithms used, details of which are available to the Requesting Agency. In its IDSAs with DIBP and AFP and DFAT, DIBP has undertaken to notify these agencies of any changes to the matching agreed parameters. In the event of a dispute over matching results, the IDSAs between DIBP and requesting agencies make it clear that each agency relies on information provided by DIBP at its own discretion, and that DIBP has no responsibility for another agency's reliance on information provided by DIBP via the FVS.