National Facial Biometric Matching Capability

Privacy Impact Assessment:

DFAT Access to DIBP Face Verification Service (Retrieve Function) for Citizenship & Visa Images

Version 1.4.1

Stephen Wilson
Lockstep Consulting
August 2016

Consulting report

NFBMC FVS Retrieve Function PIA

Version 1.4.1

For National Facial Biometric Matching Capability

[Lockstep NFBMC PIA Report 1 - Retrieve Function DIBP-DFAT (1.4.1)]

Stephen Wilson

ABN 17 582 844 015

PUBLIC

Lockstep Consulting (est. 2004) provides independent research, analysis and advice on digital identity, privacy, cyber security policy and strategy, and e-business risk management.

http://lockstep.com.au

Table of Contents

Executive Summary

Lockstep Consulting was engaged by the Attorney-General's Department to undertake a set of Privacy Impact Assessments on the different functions of the Face Verification Service (FVS) within the National Facial Biometric Matching Capability. Lockstep was asked to evaluate any privacy impacts that may be associated with the proposed use of the different FVS functions in which the Department of Immigration and Border Protection (DIBP) will provide facial biometric data and/or match results in response to requests from the Department of Foreign Affairs and Trade (DFAT) or the Australian Federal Police (AFP).

Four reports were commissioned at this stage:

1. FVS *Retrieve* function between DIBP and DFAT (this report);
2. FVS *Retrieve* function between DIBP and the AFP;
3. FVS *Match* and *Search* function between DIBP and DFAT;
4. FVS *Match* and *Search* function between DIBP and the AFP.

The scope of this first PIA is restricted to the *Retrieve* functionality being piloted by DIBP and DFAT.

The NFBMC's general objective is to utilise the considerable facial biometric holdings across government to prevent fraud, support law enforcement, promote community safety and streamline service delivery, such as assisting DFAT staff to confirm the identity of naturalised citizens applying for a passport or other travel documents. The NFBMC is a key initiative under the *National Identity Security Strategy* and the *National Biometric Interoperability Framework*. The NFBMC program is designed to enhance the ability of authorised government agencies to share and match facial images against the records of other participating agencies in a more secure, automated and accountable way than current manual processes. In the longer term, one-to-many searching for facial *identification* is planned; however the initial rollout is deliberately restricted to the less contentious functions of image retrieval and one-to-one *verification*.

The FVS is architecturally similar to the Document Verification Service (DVS); each is supported by a central hub service which provides a uniform set of interfaces whereby agencies that hold identity data can provide extracts of that data on request to other authorised agencies. The hub will retain no Personal Information in these transactions, but it will log the fact of each inquiry, and it will enforce strict access arrangements that must be struck between all participating agencies. From a regulatory perspective, the current FVS functionality will not entail any changes to the rules for sharing biometric data between DIBP and DFAT.

Overall we find that use of the FVS to share citizenship and visa related data between DIBP and DFAT as envisaged will likely be privacy positive, once it is implemented and starts to supersede today's disparate, ad hoc and sometimes under-documented inquiry methods.

Glossary

Personal Information

Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

Sensitive Information

(a) information or an opinion about an individual's:
- (i) racial or ethnic origin; or
- (ii) political opinions; or
- (iii) membership of a political association; or
- (iv) religious beliefs or affiliations; or
- (v) philosophical beliefs; or
- (vi) membership of a professional or trade association; or
- (vii) membership of a trade union; or
- (viii) sexual preferences or practices; or
- (ix) criminal record;

that is also Personal Information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

Acronyms

AFP	Australian Federal Police
AGD	Attorney-General's Department
API	Application Programming Interface
APO	Australian Passport Office
APP	Australian Privacy Principle
DFAT	Department of Foreign Affairs and Trade
DIBP	Department of Immigration and Border Protection
DIAC	(Former) Department of Immigration and Citizenship
DVS	Document Verification Service
EOI	Evidence of Identity
FIS	Face Identification Service
FVS	Face Verification Service
ICSE	Integrated Client Services Environment system
IDSA	Interagency Data Sharing Agreement

IDSS	Identity Data Sharing Service
IGA	Intergovernmental Agreement [on Identity Verification and Related Services]
IP	Internet Protocol
IPP	Information Privacy Principle (now obsolete)
IRAP	Infosec Registered Assessors Program
ISM	Information Security Manual
LACS	Logical Access Control System
LEA	Law Enforcement Agency
MD5	Message Digest number 5 (a hash algorithm)
NFBMC	National Facial Biometric Matching Capability
NISS	National Identity Security Strategy
OAIC	Office of the Australian Information Commissioner
PACS	Physical Access Control System
PIA	Privacy Impact Assessment
PICS	Passport Issue and Control System
POI	Proof of Identity
PSPF	Protective Security Policy Framework
SDLC	Software Development Lifecycle
SRMP	Security Risk Management Plan
TRA	Threat & Risk Assessment

The Australian Privacy Principles in brief

APP 1: Open and transparent management of Personal Information
APP 2: Anonymity and pseudonymity
APP 3: Collection of solicited Personal Information
APP 4: Dealing with unsolicited Personal Information
APP 5: Notification of the collection of Personal Information
APP 6: Use or disclosure of Personal Information
APP 7: Direct marketing
APP 8: Cross-border disclosure of Personal Information
APP 9: Adoption, use or disclosure of government related identifiers
APP 10: Quality of Personal Information
APP 11: Security of Personal Information
APP 12: Access to Personal Information
APP 13: Correction of Personal Information.

Introduction

Lockstep Consulting was engaged by the Attorney-General's Department to conduct a set of Privacy Impact Assessments on the design of the Face Verification Service (FVS) component of the National Facial Biometric Matching Capability. The program plans to roll out successively more complex FVS functionality through 2016, starting with image retrieval and progressing to image verification and image search, and is seeking to understand the privacy implications in an incremental manner.

Scope

This PIA Report 1 examined the information flows and privacy impacts of DFAT making inquiries against DIBP's citizenship and visa data holdings, including its facial image stores.

Approach and Methodology

This assessment involved a desktop review of NFBMC project documentation, requirements analysis, architectural details and the recently conducted preliminary hub design PIA [7], followed by group interviews with AGD, DIBP, AFP and DFAT personnel. Additional desk top review of cited materials, and several rounds of questions-and-answers followed. The PIA was conducted by Stephen Wilson, Principal Consultant, Lockstep Consulting.

Reference frame

The PIA was conducted under the Australian Privacy Principles (APPs) set out in the *Privacy Act 1988*.

Important disclaimer

The consulting advice in this document does not constitute legal advice, and should not be construed or relied upon as legal advice by any party. Lockstep Consulting is not a law firm. No legal professional privilege applies to this report.

Description of the project

Overview

The National Facial Biometric Matching Capability (NFBMC) is intended to "help government agencies combat identity crime, organised crime and terrorism. It aims to enable law enforcement and selected government agencies to share and match photographs on identity documents such as passports or other travel documents to strengthen identity-checking processes, while maintaining strong privacy safeguards"[22]. Name-based identity checking has recently been named in the Martin Place Siege Inquiry as a major problem, and biometrics have the potential to improve policing and crime prevention [21].

AGD plans a staged rollout of NFBMC functionality through 2016-17, and an incremental series of PIAs. The initial PIA has recently been completed and published [7].

The NFBMC will provide services to approved participating agencies. Participants will be required to comply with rigorous business rules and technical standards. Access to the NFBMC online services will be restricted to identified individuals within those agencies. Most access will be manual; little automated (programmed or scripted) access is envisaged at this stage. We discuss this in more detail below.

The project is assessing the privacy impacts of the Face Verification System and its three principal functions: *Retrieve*, *Match* and *Search*. Initial deployment is restricted to three agencies: DFAT and the AFP as major users of facial biometric data (in passport or other travel document processing and in investigations respectively), and DIBP as a major source of facial image data. This PIA report is one of four in a set, covering the FVS *Retrieve* function use case of DIBP providing citizenship and visa related data to DFAT. The other three reports will address FVS *Retrieve* for DIBP to AFP, FVS *Match* and *Search* functions between DFAT and DIBP, and FVS *Match* and *Search* functions between AFP and DIBP.

Privacy Context

There is an existing data sharing arrangement in place between DIBP and DFAT in relation to citizenship and visa data, which is used by DFAT as part of the passport or other travel document issuance process.

Most credential issuing, law enforcement and national security agencies collect, use and seek to match facial biometric data as part of their operations. The sharing of facial biometric and associated identifying information between Commonwealth, state and territory agencies via the FVS will be governed by a proposed Intergovernmental Agreement on Identity Matching Services (IGA). Pursuant to the IGA, participating agencies will need to comply with an FVS Access Policy and enter into

interagency data sharing agreements that meet requirements set out in the FVS access policy.

The FVS will automate the retrieval and matching of facial images, and ultimately also the searching for images associated with a particular individual.[1] The FVS will not expand agencies' powers to deal with biometrics or other Personal Information, and will not at this stage affect their current biometric collection practices or holdings. DIBP and DFAT will need legal authority to collect, use and share facial images and related Personal Information, exactly as they have needed to date.

NFBMC philosophy

The biometric matching capability is being architected according to a number of expressly privacy enhancing functions, as follows.

— Use of the new hub will only come after establishing the legal necessity and justification for use of biometrics by the participating agencies

— Formal bilateral data sharing agreements (IDSAs) are required between each pair of holding and inquiring agencies; AGD has developed a template agreement [2].

— Further, a PIA and Security Risk Management Plan must be completed by each participating agency and submitted to AGD before access will be allowed.

— No Personal Information will be retained at the hub. Minimal audit logs will be retained sufficient for oversight purposes to be able to unambiguously show which agency users performed which actions using the FVS (see also discussion of the image hash values below). Agencies will remain responsible for their own logging, and for determining what Personal Information they will log, as they must now.

— NFBMC functionality will be rolled out in stages and be restricted to a few agencies, starting with the minimum services among DFAT and DIBP as covered by this PIA, and then progressing to the steadily more sophisticated functions of *Match* and *Search*. AGD recognises that privacy concerns mount with face image search, and will address those concerns with a dedicated PIA. The NFBMC will incorporate the privacy lessons of each stage into the next.

1 Note that the future Face Identification Search (FIS) functionality remains to be fully specified and is outside the scope of the current PIAs.

— Agencies retain policy responsibility for template matching. The technical details of biometric processing and matching (which are evolving rapidly) will properly remain the business of agencies. The detailed needs of requestors and the ability of holding agencies to help with them, are matters to be negotiated and supported by agencies, without involving AGD nor the NFBMC.

The NFBMC will not be used for minor offences such as littering or parking infringements.

The hub concept

To enhance privacy, the NFBMC follows a 'hub-and-spoke' architecture pattern. This approach avoids a large central database, and has been successfully used by the national Document Verification Service (DVS), which is also operated by AGD. The NFBMC's central Interoperability Hub will not collect or store any biometric or biographic information, nor will it perform any matching. All matching occurs within the participating agencies that operate their own facial matching technology. The hub will simply broker secure, automated and auditable sharing of facial images and related data between the Participating Agencies. The hub will operate within existing privacy legislation, and agencies using the system will need to have the legislative authority to collect, use, store and disclose facial images, just as they do currently.

NFBMC should lead to consistent, auditable access to biometric matching, and (eventually) searching services, for an agency with a need to check a facial image on hand, against faces held by another agency. Crucially, the NFBMC hub will not perform any matching itself; all biometrics operations, processing and accountabilities will remain with responsible agencies. This demarcation of responsibilities creates strong PI Collection and Use limitations.

The NFBMC will save agencies from needing to create and maintain redundant agency-to-agency biometric matching interfaces. Importantly however, it does not remove the need for inter-agency agreements; these will be one of the most important privacy protection planks of the new system.

Note that every request must be directed to a specific holding agency, with a data sharing agreement already in place and provided to AGD. Any request to the hub that tries to access data at an agency where there is no data sharing agreement in place with the requestor, or where the other mandatory security and privacy arrangements are not in place (per [1]) will be automatically rejected by the hub.

No Personal Information will be retained at the hub (see also APP assessment below). Minimal details about an individual will be cached (held in temporary memory) during a session in which incoming requests are services by a holding agency; at the end of the session, the cache is purged and a minimal amount of non-identifying data is logged for the purposes of monitoring and oversight. Personal information is only used at the hub itself in order to transform data between agency formats. The NFBMC architecture essentially passes through data from requesting agency to the holding agency and back again. See APP 6 assessment below for further details.

The logging of photo hash values

The hub will retain in its audit logs a hash value of every photograph that is returned for each *Retrieve* request. The purpose of this collection is to allow investigation when necessary of the exact data that flowed for any given transaction with the hub. The technical nature of a hash value (calculated by an algorithm such as MD5 in the case of the NFBMC currently) is that the hashed data is unique to the original photo concerned but cannot be used to reconstruct that photo. The hash is sometimes referred to as a "thumbprint", for it is unique to the photo. In the event of any change to or substitution of the photo, the re-calculated hash value will always be different. No two photos, even of the same person taken at the same time under identical circumstances will ever generate the same hash value, thanks to the sensitivity of the algorithm. The purpose of the hash is to prove that a given photo was involved in a given NFBMC transaction. Without the given original photo, the hash cannot be used to reconstruct any Personal Information.

Security and access controls

Multiple layers of logical access control are included in the design to tightly lock down access to authorised personnel [3]. Authentication mechanisms include username and password, an X.509 digital certificate issued by AGD only to named authorised agency users, and IP address white-listing (whereby the precise office location of each authorised user's computer is known to the hub access control system; attempts to gain entry, even by legitimate users from unexpected locations, will be blocked).

Training and management of FVS users

Access to the FVS will only be provided to a limited number of nominated users from requesting agencies, restricted to employees of those agencies who have a reasonable need to use the FVS to fulfil the functions of their employment. Agencies will manage the number of nominated users and maintain user records which will be subject to audits.

Nominated users will be required to undertake training on privacy, security and interpreting the results of the FVS. Access to DIBP's FVS *Retrieve* function will only be provided to APO staff that have been trained in facial recognition.

Hub connection options

Agencies participating in the FVS may connect to the hub via one of two means: a web-based portal for human users and automated system-to-system connections.

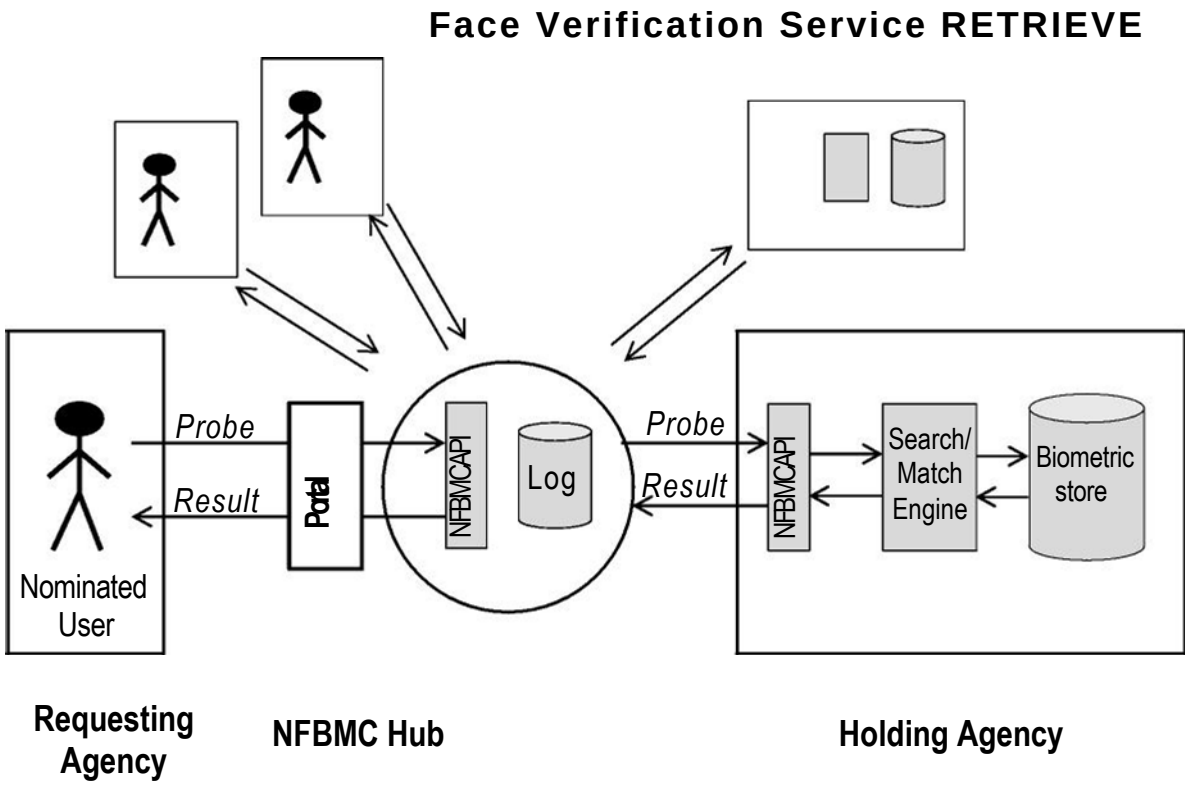
The portal enables nominated users to submit queries individually, entering data manually. While queries are submitted manually, the response from the holding agency will be automated and returned via the portal.

There will be a number of APIs for agencies to establish system-to-system connections with the hub. These will enable agencies to automate the submission of queries via the hub, either individually or in batches. This will enable agencies to incorporate an automated FVS query as part of a standard business process that requires verification of a person's identity, for example processing passport or other travel document applications. System-to-system connections will operate within appropriate access permissions and privacy controls, with auditability similar to human users. AGD envisages that most if not all agencies using the FVS will use the portal in the first instance, before adopting a system-to-system connection over time.

The FVS *Retrieve* function

The following figure depicts the FVS hub-and-spoke architecture, through which a nominated user at a requesting agency may direct a retrieve request to a holding agency, and have responses returned, via the interoperability hub portal.

In future, these APIs will be exposed for use in automated system-to-system connections between the requesting agency and the hub. Initially however, DFAT's access to DIBP's FVS *Retrieve* function will only be implemented in a manual mode using the hub portal.



Only one of six APIs designed into the hub is relevant to this PIA: *RetrieveBiometricRequest*. [2] This function takes an identity document type (a Citizenship Certificate or visa) and document number, family name and date of birth (plus optionally a given name) and returns a facial image (if one is available) and corresponding biographic details from the Holding Agency (DIBP) [4].

[2] Other APIs for matching a given facial image and for identifying a given image, will be subject to PIAs reports 3 and 4.

Information flow mapping

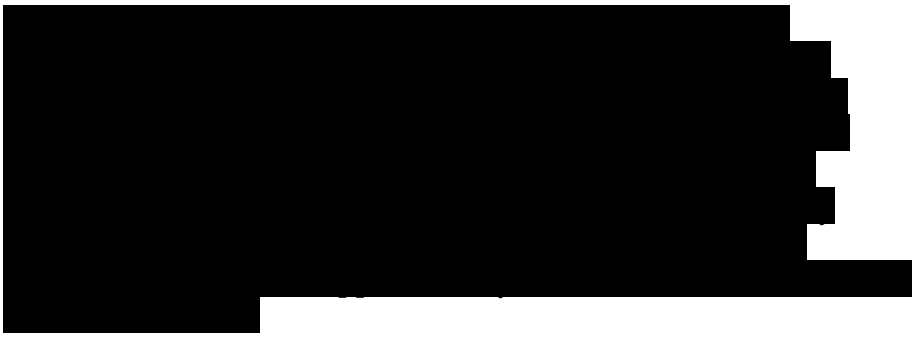
Existing flows

Citizenship

There are currently, three separate channels for the exchange of citizenship information from DIBP to DFAT:

1. Automated daily extract of persons who have been approved, acquired or lost citizenship.
2. Automated disclosure of facial images of persons who have been approved or acquired citizenship.
3. Manual ad hoc requests for citizenship verification on specific individuals who have applied for an Australian passport or other travel document.

1. Automated daily extract



2. Automated disclosure of citizenship facial images

3. Manual ad hoc requests for citizenship verification

A third manual flow of information from DIBP to DFAT occurs on an ad hoc basis, where DFAT officers contact DIBP's Citizenship Help Desk to seek confirmation of the identity and/or citizenship status of persons applying for an Australian passport. [redacted]

Visa

Currently DFAT's access to visa data is limited and occurs through manual processes on an ad hoc basis. DFAT requests visa data from DIBP for the purposes of checking the visa status of people applying for a Conventional Travel Document (CTD) or Certificate of Identity (COI). At present there are approximately 2000 such cases per year.

Future flows

APO's approved operators will use the *Retrieve* function to manually bring up the citizenship or visa photo of a passport applicant whose identity has not been matched automatically by way of future processes. [redacted]

High level privacy analysis

Before detailed assessment against the APPs in the next chapter, we summarise the major issues as seen by Lockstep.

NFBMC privacy & security framework

The privacy of the FVS rests on a number of security and data protection measures laid out the in the FVS access policy [1]. Here we summarise and annotate those measures (each of which must be lodged as a document with AGD, unless otherwise noted).

— **Statement of Legislative Compliance** setting out the regulatory justification for the transfer of biometric data between each agency involved.

— **Privacy Impact Assessments** will be required for each agency joining the hub.

— **Management of Nominated Users** within each participating agency will be via multifactor authentication, and will be logged and auditable at the individual transaction basis. Some minimal logging (or unique transaction ID, time and date) will be done at the hub; the larger share of event logging anticipated to be needed for reasonable oversight, shall be the responsibility of the agencies.

— **Security and Privacy Awareness** training will be required for all nominated agency users.

— **Auditing and Accountability**: Agencies will be required to audit their use of the FVS at least annually. AGD's intention is to require audits to be sufficiently detailed as to uncover the time and date, the purpose, and the requesting user for each transaction.

— **Interagency Data Sharing Agreements** (IDSAs) must be established between all pairs of agencies using the FVS. AGD plans to provide a template IDSA.

— **Transparency**: the PIAs, data sharing agreements (ISDAs) and the statement of legislative compliance will all be published, to the greatest extent possible, allowing for security or other reasons preventing full publication.

— **Security Accreditation**, against the PSPF and ISM, of all systems connected to the hub.

— **Service Level Agreement** with the Attorney-General's Department.

Assessment against the APPs

In this section we examine the compliance of the FVS *Retrieve* function, operating between DIBP and DFAT, with the 13 APPs.

APP 1: Open and transparent management of Personal Info

Assessment & Findings

DFAT is open and transparent in its handling of facial biometrics, insofar as it plainly sets out (on its forms) the legislated basis for collecting face data from passport applicants. Technically, the FVS does not affect the collection notices provided by DFAT to passport applicants.

DIBP has practices and procedures to ensure compliance with the requirements of all APPs, including APP 1 which requires a clearly expressed and up-to-date Privacy Policy about how Personal Information is managed. The Privacy Policy details how DIBP manages the Personal Information it collects and the information flows associated with that personal information. The Privacy Policy informs individuals how they may lodge a complaint if they believe DIBP has wrongly collected or handled their personal information. DIBP maintains a privacy notice, Form 1442i, *Privacy notice* [17], which includes matters required under APP 1 and APP 5 of which DIBP must advise persons when collecting their personal information, including personal identifiers. DIBP advises that, if individuals are not satisfied with DIBP's response, they are advised that it is open to them to contact the Australian Privacy Commissioner.

DIBP also has a separate notice, Form 1243i, '*Your personal identifying information*' [19], which explains DIBP's authority to collect personal identifiers, how they may be collected, the purposes of collection and the purposes for which they are permitted to be disclosed. Form 1243i is publicly available on the Department's website.

APP 2: Anonymity and pseudonymity

Assessment & Findings

Anonymity is not generally relevant to DFAT use cases such as passport or other travel document applications. It is generally understood by citizens (and they are reminded through statements in the passport or other travel document application forms) that they must be identified to interact meaningfully with DFAT. The FVS makes no change to the way DFAT uses biometrics nor the applicability of anonymity or pseudonymity.

Sections 17(3), 19D(4), 24(3), 30(3), 33(4) and 37(4) of the *Australian Citizenship Act 2007* (the Citizenship Act [16]) require that, before an application is approved, the Minister must be satisfied of the person's identity. If a person's identity cannot be verified the application cannot be approved.

Division 5 of Part 2 of the Citizenship Act provides the legislative framework for collecting personal identifiers from people seeking to sit a test, or applying for Australian citizenship or evidence of Australian citizenship. The individual is advised of this via Form 1243i [19].

Any personal information that DIBP collects or discloses to DFAT is for the purpose of authenticating identity. As such anonymity or pseudonymity is not applicable.

Therefore APP 2 is not activated, and we make no recommendations here.

APP 3: Collection of solicited Personal Information

Assessment & Findings

The hub does not solicit any information at all as such, but only passes through Personal Information of individuals of interest to DFAT officers for specific purposes expressly sanctioned by law, for the purposes of processing passport or other travel document applications and related functions. No Personal Information persists in the FVS systems or audit logs. The individuals involved in FVS transactions cannot be reasonably identified from the transaction IDs and photo hashes and therefore APP 3 is not activated.

Through its use of the FVS, DFAT will continue to collect Personal Information from DIBP (as it does now) for the purposes of processing passport or other travel document applications made by those individuals. Over time, the volume of this Personal Information flow is expected to decrease as a result of more targeted inquiries being made possible.

We have no recommendations to make in relation to APP 3.

APP 4: Dealing with unsolicited Personal Information

Assessment & Findings

Under section 6 of the *Privacy Act 1988*, an entity solicits personal information if it requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included. As DIBP will provide citizenship and visa related images and biographic data to DFAT via the *Retrieve* function of the FVS solely on a query-and-response basis, DFAT will receive only personal information that is has *solicited*.

The hub of course handles, fleetingly, Personal Information that the Hub itself did not solicit, passed through by participating agencies. The hub merely provides a conduit for passing certain Personal Information between agencies, which have signed up to the FVS Access Policy, and which must have legal basis for handling that Personal Information regardless of the hub. The FVS by design minimises the Personal Information exchanged between agencies and structures that information through the FVS hub. The express role of the hub is to reduce the ad hoc

exchange of biometric data, by providing easier to use and easier to audit formal automated channels. Data retained in hub audit logs are not identified, containing only an externally meaningless transaction code, and are not reasonably identifiable.

As DIBP will provide citizenship and visa related images and biographic data to DFAT via the *Retrieve* function of the FVS solely if there is a match, DFAT will receive only personal information that it has *solicited*.

Therefore we have no recommendations to make in relation to APP 4.

APP 5: Notification of the collection of Personal Information

DIBP currently collects photos and biographic data from citizenship applicants as part of the application process, in accordance with the *Australian Citizenship Act 2007* [16], and from visa applicants in accordance with the *Migration Act 1956* [17]. At the time a citizenship or visa application is made, the applicant is notified by information on the application form, of matters required by APP 5.2(b), including any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which DIBP usually discloses personal information of the kind collected, such as DFAT.

In accordance with APP 5, DIBP must notify individuals from whom it collects personal information about a number of matters. These matters are addressed in several departmental forms as well as the DIBP Privacy Policy. Form 1243i [19] explains DIBP's authority to collect personal identifiers from citizenship and visa applicants (among others), how they may be collected, the purposes of collection, how they may be used, how they will be protected and how they may be disclosed.

Then as part of the passport or other travel document application process, DFAT notifies applicants via the application form that they submit, that DFAT may collect information about the applicant from other government agencies to verify the applicant's citizenship status, thereby discharging its obligations under APP 5.2(b).

The FVS does not change the purposes for which DFAT collects or the way it uses biometric data, but instead delivers individuals' facial images to authorised DFAT officers in a more secure, more accountable manner. Therefore, existing notification practices by DIBP and DFAT appear sufficient for FVS *Retrieve* to satisfy APP 5.

We have no recommendations to make in relation to APP 5.

APP 6: Use or disclosure of Personal Information

In a limited sense, the hub can be regarded as *using* Personal Information, insofar is it transforms some parameters sent in as part of a retrieval request so they may be passed through to a holding agency for processing. For completeness, Lockstep regards that use as fitting the purpose of the

hub. For the DIBP-DFAT use case, no Personal Information will ordinarily be disclosed by the FVS to any entity beyond DFAT .

Once FVS delivers an image into an inquiring agency' systems (at DFAT in this case), the potential re-use of that image and other Personal Information can only be constrained by legal agreements. The IDSA between DIBP and DFAT, structured according to the template provided by AGD [2], will enjoin DFAT to limit the way it uses facial data obtained via the FVS, in line with the agencies' legislative obligations. This is an appropriate mechanisms in Lockstep's opinion, [redacted]

Section 43(2)(e) of the *Australian Citizenship Act 2007* [16] permits the disclosure of identifying information under an arrangement entered into with an agency of the Commonwealth, or with a State or Territory, or an agency of a State or Territory, for the exchange of identifying information. The definition of identifying information (in s 3 of the Act) encompasses citizenship and visa personal identifiers.

If a retrieval request sent by DFAT results in a match against DIBP's holdings based on meeting agreed parameters, then the personal information and facial image, where available, will be returned to DFAT. This information will enable DFAT to authenticate an individual's identity, and combat document and identity fraud.

The disclosure of citizenship- and visa-related data including images by DIBP to DFAT is permitted under APP 6.2(e) as it is reasonably necessary for DIBP's enforcement related activities. Specifically, DIBP's functions and activities, covered by the 'enforcement related activity' exceptions in APPs 3.4(d)(i), 6.2(e) and 8.2(f), include cooperation with other agencies, including information-sharing, for law enforcement and border security purposes, and the protection of public revenue.

We have no recommendations regarding APP 6.

APP 7: Direct marketing

Assessment & Findings

Direct marketing is not applicable. Therefore APP 7 is not activated for the purposes of this PIA.

APP 8: Cross-border disclosure of Personal Information

Assessment & Findings

There is no cross-border flow of Personal Information in the anticipated operation of the FVS by DFAT and DIBP. The only users of the FVS in the DIBP-DFAT pilot are APO officers processing passport or other travel document applications in Australia.

We therefore make no findings or recommendations with respect to APP 8.

APP 9: Adoption, use or disclosure of government identifiers

APP 9 applies to adoption, use or disclosure of government identifiers by an "organisation", which is defined in section 6C of the *Privacy Act* to exclude an "agency". Under s 6 of the *Privacy Act*, an "agency" includes a Department. Therefore, neither DFAT nor DIBP are organisations for the purposes of the Privacy Act, and APP 9 does not apply to DFAT's and DIBP's adoption, use or disclosure of government identifiers.

Thus we find that APP 9 will not be activated by the use of the FVS *Retrieve* function by DIBP and DFAT, and so we make no findings or recommendations with respect to APP 9.

APP 10: Quality of Personal Information

Assessment & Findings

The FVS plays no direct part in the quality of biometric data holdings at any agency. In respect of APP 10, the hub is neutral.

It could be argued that the use of the FVS should, over time, lead to improved quality in DFAT's biometric holdings, through better detection of discrepancies and more targeted usage. It is difficult to generalise at this time and we leave it to other agency-specific PIAs in future, under the NFBMC participation arrangements, to evaluate the possible improvements to quality that the hub might facilitate.

APP 11: Security of Personal Information

Assessment & Findings

The FVS system has been subject to standard risk assessment, as a matter of course, and will be reviewed and reviewed by an IRAP assessor and approved by the AGD IT Security Advisor in accordance with the ISM. A condition of the FVS access policy is that the DIBP and DFAT systems also be IRAP-assessed. With Personal Information only transiting the system (not remaining in the system) and following pathways that are better defined and controlled than the current manual biometric handling processes, Lockstep considers that the security of Personal Information should be much enhanced by the FVS.

When DFAT sends a request via the Hub, this fact will be recorded in an audit log. The audit log also displays the status of that request, that is, pending, no match, or match. Following a match, a summary of information (without any Personal Information of the individual concerned) sent via the Hub is also recorded in the FVS audit log.

We find that APP 11 is satisfied by the FVS *Retrieve* function to be implemented at DFAT and DIBP. We have no recommendations.

APP 12: Access to Personal Information

There is no Personal Information retained in the Hub supporting the FVS, only meaningless transaction IDs held in the audit logs.

We find that APP 12 is not activated and therefore we make no recommendations.

APP 13: Correction of Personal Information

Assessment & Findings

Further to the APP 12 assessment above, APP 13 is not activated by the FVS. It may be noted that by improving and formalising the use of biometric matching between agencies, the FVS (and NFBMC more broadly) has some potential to improve compliance with APP 13 by participating agencies. This should be evaluated by detailed agency specific PIAs in future.

Conclusions

We conclude that the Face Verification Service – as exemplified by the DFAT-DIBP use case covered in this Report 1 – should bring an important improvement to the privacy of biometric data processed by government. Facial biometric data is a critical asset for processing passport or other travel document applications, and, in the longer term, for ensuring national security and combating fraud. It is a reality that biometric data will be used more widely and more deeply in coming years. It is timely for the FVS to be introduced chiefly as a means to constrain and control the flow of facial data.

Lockstep finds that the FVS is likely to improve privacy in the data sharing arrangements between DIBP and DFAT in the following broad ways:

— The FVS will, over time, reduce the exposure of biometric data, by helping DIBP and DFAT shift from ad hoc data transfers to more specific transactions, on a need-to-know basis.

— The FVS will formalise the handling of biometric data by restricting functionality to the specific agencies and named staff members who meet stringent security and privacy requirements as set out in the FVS access policy [1].

We note that the bulk flows of facial biometric data between DIBP and DFAT will not be reduced by the FVS *Retrieve* function. A positive impact for these agencies will come later from changes to the passport or other travel document application process to make use of automated *Match* and *Search* functions, which will be studied in a subsequent PIA.

Recommendations

For the operation of the initial, portal-based Face Verification Service pilot being conducted between DIBP and DFAT for the retrieval of citizenship and visa related images, no recommendations arise from this PIA.

Beyond this initial service, when the FVS APIs are exposed, we recommend that a further privacy analysis be done on the system-to-system functionality, and the impact on overall Personal Information flows.

Note that further PIAs on the FVS *Match* and *Search* functions will follow this report.

References

Project documents

[1]. *FACE VERIFICATION SERVICE ACCESS POLICY*, Draft (undated), Attorney-General's Department
Filename: Facial Verification Service Access Policy.pdf

[2]. *Interagency Data Sharing Agreement* [template] V3.1, 24 March 2016 National Facial Biometric Matching Capability Face Verification Service
Filename: Meeting paper - Item 2(d) - Attachment B - FVS IDSA template - Programme Advisory Committee - 7 April 2016.docx

[3]. *Face Matching Services*, (undated), Attorney-General's Department
Filename: Fact-Sheet-National-Facial-Biometric-Matching-Capability.pdf

[4]. *Interoperability Hub Technical Concept of Operations*, Attorney-General's Department, October 2015
Filename: Technical Concept of Operations.docx

[5]. *'Verification -> Retrieve' Function - DIBP Citizenship Data*, Attorney-General's Department, V0.5, 15th Jan, 2016
Filename: Business Requirements - Retrieve Function - DIBP Citizenship Data - V0.5....docx

[6]. *Identity Hub: System Access Flows,* Draft v0.4 April 2015
Filename: MASTER - AGD Access Maps DRAFT v0.4.pdf

[7]. *National Facial Biometric Matching Capability Privacy Impact Assessment – Interoperability Hub*, Information Integrity Solutions, August 2015
https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Privacy-Impact-Assessment-National-Facial-Biometric-Matching-Capability.PDF

[8]. *Department of Foreign Affairs Privacy Policy*
http://dfat.gov.au/about-us/about-this-website/pages/privacy.aspx

[9]. *Concept of Operations National Facial Biometric Matching Capability* v0.7
Filename: Concept of Operations - National Facial Biometric Matching Capability - .pdf

[10]. *Blueprint National Facial Biometric Matching Capability* (undated),
Filename: Master Blueprint - National Facial Biometric Matching Capability - Nov 2...pdf

[11]. *Basis for DIBP to disclose Identity Information to DFAT AFP*, Duncan Anderson, Attorney-General's Department, by email, 19th January, 2016.

[12]. *DIAC Project Privacy Impact Assessment*, Dept of Immigration and Citizenship Identity Branch, 11 November 2009
Filename: DIAC DFAT Exchange of Identity Data Part A - PIA v0.13

[13]. *Draft IPP Audit Report: DIAC Exchange of identity data through the Systems for People project*, Office of the Privacy Commissioner, March 2010
Filename: Audit - 2010-03 DIAC SfP Draft Audit Report amac.doc

Agency documents

[14]. *DFAT/AEC Batch Suite*
Filename: DFAT AEC Extract.xlxs

External References

[15]. *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)*

[16]. *Citizenship Act 2007 (Cth)*
http://www.austlii.edu.au/au/legis/cth/consol_act/aca2007254/

[17]. *Migration Act 1958 (Cth)*
http://www.austlii.edu.au/au/legis/cth/consol_act/ma1958118/

[18]. *Privacy notice* form 1442i, Department of Immigration and Border Protection
https://www.border.gov.au/Forms/Documents/1442i.pdf

[19]. *Your personal identifying information* form 1243i, Department of Immigration and Border Protection
https://www.border.gov.au/Forms/Documents/1243i.pdf

[20]. *Australian Privacy Principles guidelines*, Office of the Australian Information Commissioner, V1.0, February 2014
http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf

[21]. *Martin Place Siege: Joint Commonwealth - New South Wales review,* Department of Prime Minister and Cabinet, and NSW Premier and Cabinet, January 2015
https://www.dpmc.gov.au/sites/default/files/publications/170215_Martin_Place_Siege_Review_1.pdf

[22]. *New $18.5 million biometrics tool to put a face to crime,* Minister for Justice, Media Release, 9 Sept 2015

[23]. *Document Verification Service Privacy Policy* (accessed 14 Jan)
http://www.dvs.gov.au/Pages/Disclaimers/Privacy-statement.aspx