



National Facial Biometric Matching Capability

Privacy Impact Assessment:

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

Version 1.2.1

Stephen Wilson
Lockstep Consulting
August 2016

Consulting report
NFBMC FVS Retrieve Function PIA
Version 1.2.1
For National Facial Biometric Matching Capability
[Lockstep NFBMC PIA Report 2 - Retrieve Function DIBP-AFP (1.2.1)]

Stephen Wilson

Copyright © 2015-16 Lockstep Consulting

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	4
Glossary	5
Introduction	7
Scope	7
Approach and Methodology	7
Important disclaimer	7
Description of the project	8
Overview	8
Privacy Context	8
NFBMC philosophy	9
The hub concept	10
The logging of photo hash values	11
Security and access controls	11
Training and management of FVS users	11
Hub connection options	12
The FVS <i>Retrieve</i> function	12
Information flow mapping	14
Existing flows	14
High level privacy analysis	15
NFBMC privacy & security framework	15
Assessment against the APPs	16
APP 1: Open and transparent management of Personal Info	16
APP 2: Anonymity and pseudonymity	16
APP 3: Collection of solicited Personal Information	17
APP 4: Dealing with unsolicited Personal Information	17
APP 5: Notification of the collection of Personal Information	18
APP 6: Use or disclosure of Personal Information	18
APP 7: Direct marketing	20
APP 8: Cross-border disclosure of Personal Information	20
APP 9: Adoption, use or disclosure of government identifiers	20
APP 10: Quality of Personal Information	20
APP 11: Security of Personal Information	21
APP 12: Access to Personal Information	22
APP 13: Correction of Personal Information	22
Conclusions	23
Recommendations	24
References	25

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

The scope of this first PIA is restricted to the *Retrieve* functionality being established between DIBP and the AFP.

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 document. 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 functions of one-to-one image retrieval and verification that entail lesser privacy impacts.

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 about members of the public in these transactions, but it will log the fact of each inquiry and pseudonymous usernames indicating which authorised agency users were involved, 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 legislative basis for sharing biometric data amongst DIBP and AFP.

Overall we find that using the FVS to share citizenship and visa related data between DIBP and the AFP 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

<i>Personal Information</i>	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: <ul style="list-style-type: none"> (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.
<i>Sensitive Information</i>	<ul style="list-style-type: none"> (a) information or an opinion about an individual's: <ul style="list-style-type: none"> (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
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 Matching Services]

IP	Internet Protocol
IRAP	Infosec Registered Assessors Program
ISM	Information Security Manual
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
PIA	Privacy Impact Assessment
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

- 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 2 examines the information flows and privacy impacts of AFP making *Retrieve* inquiries against DIBP's citizenship and visa data holdings, including its facial image stores through the FVS hub (while the closely related Report 1 looks at the same interface in operation between DFAT and DIBP).

The focus of this and the other three related FVS PIAs is privacy of members of the public who are subject to biometric matching transactions. Unless noted otherwise, "Personal Information" in this report means Personal Information of a member of the public, and not that of staff members using the FVS.

Approach and Methodology

This assessment involved a desktop review of NFBMC project documentation, requirements analysis, architectural details and the recently conducted initial PIA, 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” [21]. 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 [20].

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 Service 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 an initial set, covering the FVS *Retrieve* function use case of DIBP providing citizenship and visa data to the AFP. The other three reports will address FVS *Retrieve* for DIBP to DFAT, FVS *Match* and *Search* functions between DIBP and DFAT, and FVS *Match* and *Search* functions between DIBP and AFP.

Privacy Context

There is an existing data sharing arrangement in place between DIBP and the AFP in relation to citizenship and visa data, which is used by AFP in the performance of its functions, particularly criminal and national security investigations.

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). Current manual methods for requesting raw biometric data and matching services are covered by laws and

regulations, but the methods are cumbersome, may be occasionally applied inconsistently, and are difficult to oversee or audit for consistency. The timely discovery of important policing information in existing facial image stores is thus sometimes impeded. There is evidence that better sharing of facial biometrics will help law enforcement and national security [20].

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 [1].

The FVS will automate the retrieval and matching of face images, and ultimately also the searching for images,¹ leading to better “time to insight” in law enforcement activities. The FVS will not expand agencies’ powers to deal with biometrics or other Personal Information, and at this stage will not affect their current biometric collection practices or holdings. DIBP and the AFP 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 confirming the legal permissibility 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 about members of the public will be retained at the hub. Minimal audit logs will be retained sufficient for oversight purposes to be able to unambiguously show which authorised agency users performed which actions using the FVS (see also discussion of the image hash values below). Agencies will remain responsible for their own detailed event logging, and for determining what Personal Information if any they will log in their systems, 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 the AFP and DIBP as covered by this PIA, and then progressing to the steadily more sophisticated functions of *Match* and *Search*. AGD

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

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.

- 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 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 strengthens limitations on collection and use of Personal Information.

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 about members of the public will be retained at the hub (see also APPs assessment below). Minimal details about an

individual who is the subject of a *Retrieve* request 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 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. Some Personal Information about authorised agency users is logged at the hub, for audit purposes. This information is in the form of pseudonymous usernames which are not identifiable to AGD, but are identifiable when combined with other information held by the requesting agency. It should be generally understood by users of biometrics technologies in government that their usage will be monitored, as part of normal staff accountability processes.

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 [1]. 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 AFP 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.

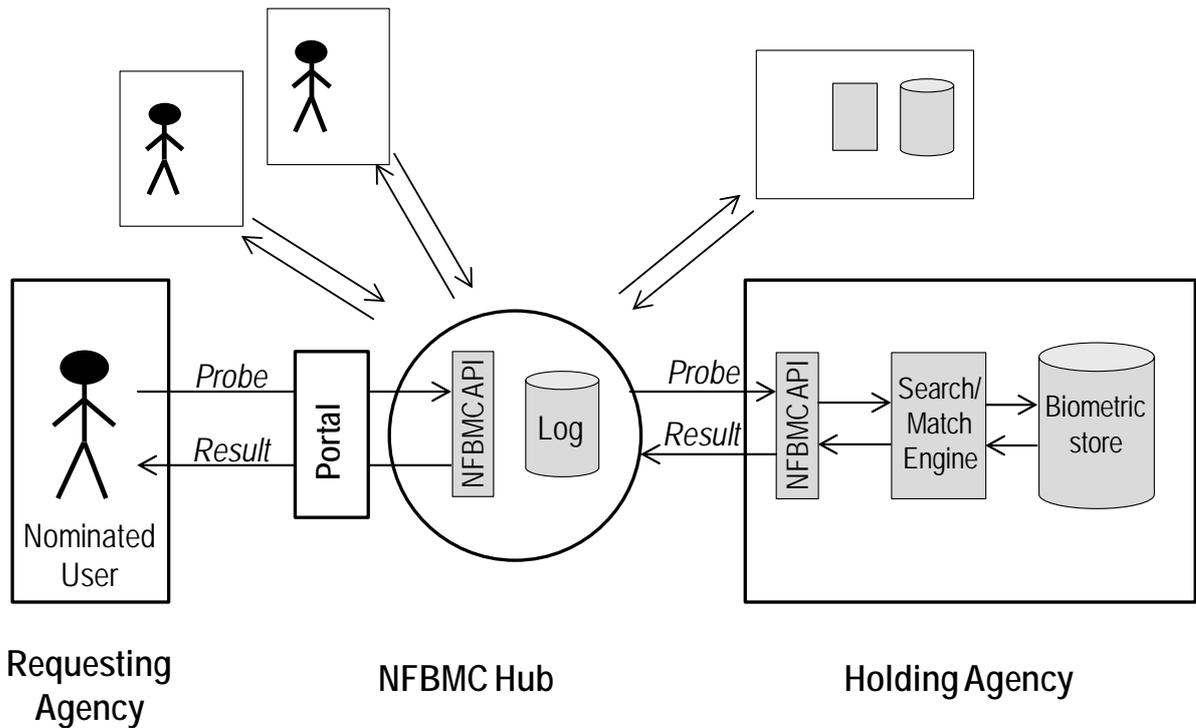
There will be a number of APIs for agencies to establish system-to-system connections with the hub. These will enable agencies to automate the submission of queries via the hub, either individually or in batches. This will enable agencies to incorporate an automated FVS query as part of a standard business 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, the AFP's access to DIBP's FVS *Retrieve* function will only be implemented in a manual mode using the hub portal.

Face Verification Service RETRIEVE



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).

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

Currently the major flows of Personal Information and face biometric-related data from DIBP to AFP are via separate inquiries initiated by officers. There is a convention that all requests lodged with DIBP by an AFP officer need to cite the reason and legal justification for obtaining the data concerned. We understand that a reference to legislation is commonly included in each request.

Requests are usually lodged by email to a shared group email box at DIBP. This habit will produce something of a uniform audit trail at such email boxes, however there is no guarantee that we can see that requests are not lodged in other channels. Further, the group email box makes it difficult to tell which DIBP staffer serviced the request.

Future flows

With the FVS, every request to retrieve information will be logged at the hub and identified by username of the requesting AFP officer. Most data will be passed straight through the hub, with some formatting transformation, but no addition or subtraction of Personal Information.

There will also be strict enforcement in the business rules implemented in NFBMC of the status of the interagency arrangements that authorise participation in the hub. In principle, it should be possible to use access control sub-systems in the hub to revoke access in the event that a participating agency should fail a periodic privacy or security audit, or have otherwise failed to comply with AGD requirements. Individual user level access control (such as blacklists or IP address white lists) could also be used without major modification to the architecture.

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 system rests on a number of security and data protection measures laid out in the FVS Access Policy [1]. Here we summarise and annotate those measures.

- **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 by username at the individual transaction level. Some minimal logging (of unique transaction ID, username, 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 cover 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 has developed a template IDSA [2].
- **Transparency:** the PIAs, data sharing agreements (IDSAs) 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 NFBMC FVS *Retrieve* function with the 13 APPs.

APP 1: Open and transparent management of Personal Info

Assessment & Findings

The AFP's use of biometric face image data at present and in the intended use of the FVS fall under the law enforcement provisions of the Privacy Act. The AFP Privacy Policy [9] provides a comprehensive account of the Personal Information and Sensitive Personal Information (including facial images and fingerprints) that the AFP may collect and why, and a list of many of the legislative mechanisms that apply, including the AFP Act [13], the *Crimes Act 1914* (Cth), the *Crimes Act 1900* (ACT) and so on.

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*' [18], 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 the AFP's law enforcement related use cases. The FVS makes no change to the way AFP uses biometrics nor the applicability of anonymity or pseudonymity. 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 AFP officers for specific purposes related to law enforcement or national security. No Personal Information about members of the public persists in the FVS systems or audit logs. The individuals that are the subject of FVS transactions cannot be reasonably identified from the transaction IDs and photo hashes and therefore APP 3 is not activated in respect of collection by the hub itself.

Through its use of the FVS, the AFP will continue to collect Personal Information from DIBP's citizenship and visa related holdings (as it does now) for the purposes of attempting to verify the identity of persons of interest. Existing laws that authorise the disclosure of Personal Information by DIBP to AFP include the *Migration Act 1958* (s 336E), the *Australian Citizenship Act 2007* (s 43) and the *Australian Border Force Act 2015* (s 44 and s 46).

Facial images used for biometric identity verification are of course *Sensitive Information* under the Privacy Act (see *Glossary* above). APP 3.4(d) enables collection of Sensitive Information without consent of the individual, by an enforcement body where that body believes that collection is reasonably necessary for, or directly related to, one or more of its functions or activities. The AFP's functions are set out in s 8 of the *Australian Federal Police Act 1979* [13]. The AFP's Privacy Policy [9] is clear about its authority under the Privacy Act and the AFP Act to collect facial images. Over time (as FVS functions beyond the initial *Retrieve* are rolled out) 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

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 a 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. Information retained in hub audit logs about individuals who are subject to FVS transactions is not identified, contains only an externally meaningless transaction code, and is not reasonably identifiable.

As DIBP will provide citizenship and visa-related images and biographic data to the AFP via the *Retrieve* function of the FVS solely if there is a match, AFP 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* [14], and from visa applicants in accordance with the *Migration Act 1956* [15]. 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 the types of organisations to which DIBP usually discloses Personal Information of the kind collected. In particular, Form 1243i [18] states:

The department is authorised to disclose your personal identifiers and information relating to your name and other relevant biographical data to a number of agencies including law enforcement ...

The FVS does not change the purposes for which the AFP collects nor the way it uses biometric data, but instead delivers individuals' facial images to authorised AFP officers in a more secure, more accountable manner. Therefore, existing notification practices by DIBP and AFP 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 as 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-AFP use case, no Personal Information will ordinarily be disclosed by the FVS to any entity beyond the AFP.

Once FVS delivers an image into a requesting agency's systems (at AFP in this case), the potential re-use of that image and other Personal Information can only be constrained by agreements. The IDSA between DIBP and AFP, structured according to the template provided by the NFBMC [2], will limit the ways that AFP can use facial data obtained from DIBP through the FVS, in line with the agencies' legislated functions.

The IDSA will provide a mechanism for DIBP to clearly articulate the circumstances under which the AFP may disclose to third parties Personal Information that it has obtained through the FVS. Currently, manual transfer of biometric data is covered by a host of MOUs between the AFP and DIBP. The IDSA, in Lockstep's opinion will be a distinct improvement on the present MOUs, as and when transfer via the FVS comes to supersede manual transfer.

Section 43(2)(e) of the *Australian Citizenship Act 2007* [14] 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 the AFP 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 the AFP. This information will enable the AFP to authenticate an individual's identity, and, amongst other things, combat fraud.

The disclosure of citizenship-related data including images by DIBP to the AFP is permitted under APP 6 with reference to s 43(2)(ea) of the *Citizenship Act* [14] as it is deemed reasonably necessary for the enforcement of the criminal law of the Commonwealth, a State or a Territory. The disclosure of visa-related images by DIBP to the AFP is permitted with reference to s 336E(2)(a)(i) of the *Migration Act* [15] as it is deemed reasonably necessary for data-matching in order to identify or authenticate the identity of a person. In principle, there is a risk that DIBP-sourced Personal Information might be put to a secondary purpose by AFP unrelated to the primary purpose of collection. The same risk is present in the current manual processes for the retrieval by AFP from DIBP of biometric and biographical data, as described above in *Information flow mapping*. The main mitigation of that risk is AFP's commitment to proper handling of Personal Information outlined in section 6(a) of the AFP Privacy Policy [9] (which also sets out the regulatory justification for AFP handling biometric data). This risk is not fundamentally altered by the introduction of the FVS and since this PIA focuses on the impact of the introduction of the FVS, we assume that existing AFP processes are compliant with the Privacy Act.

Having said that, once FVS-enabled processes are widely implemented at the AFP, the risk of inappropriate secondary usage of biometric Personal Information may be somewhat reduced as a result of the superior auditability of future data flows. It will be easier in future to determine where a given digital facial image came from and who within AFP would have retrieved the image in the first place. While the subsequent flows and usage of images within AFP are beyond the control of NFBMC and outside the scope of this PIA, the better transparency of the initial retrieval may act as an aid to the investigation of inappropriate usage should it occur, and as deterrent too.

Without implying any shortcoming in existing AFP practices, we also highlight that the additional privacy and security measures imposed by the FVS Access Policy [1] and the requisite PIAs and SRMPs should make it even less likely that inappropriate secondary use of biometric data will occur.

We have no recommendations regarding APP 6.

See also *Limiting use of the hub* in the main body of the report.

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

Any cross-border flow of Personal Information in the anticipated operation of the FVS by the AFP will be to locations under full control by the AFP, using systems and processes that comply with the APPs. Thus APP 8 will be satisfied.

In theory, there is a risk that DIBP-sourced Personal Information might be transmitted across borders to a country that does not comply with the APPs. The same risk is present in the current manual processes for the retrieval by AFP from DIBP of biometric and biographical data, as described above in *Information flow mapping*. The main mitigation of that risk is AFP's commitment to proper handling of Personal Information outlined in section 6(a) of the AFP Privacy Policy [9]. This risk is not fundamentally altered by the introduction of the FVS and since this PIA focuses on the impact of the introduction of the FVS, we assume that existing AFP processes are compliant with the Privacy Act.

We 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 AFP nor DIBP are organisations for the purposes of the Privacy Act, and APP 9 does not apply to AFP'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* by DIBP and AFP, 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 biometrics 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.

Any personal information obtained by the AFP from DIBP through the FVS will be subject to the AFP's existing obligation to take reasonable steps to ensure the quality of personal information that it uses or discloses. In addition to the AFP's existing procedures for discharging this obligation, and in accordance with the FVS Access Policy, the IDSA between DIBP and AFP is expected to contain express protections that apply to secondary use of Personal Information obtained under the new data sharing arrangements. AGD advises that these protections would require the AFP to take reasonable steps to confirm the accuracy of the information with DIBP through other means, before using the information for evidentiary purposes. This mechanism in the IDSA would reinforce existing obligations to ensure the quality of personal information collected by the AFP in cases where it is likely to have the most serious consequences for an individual.

We have no recommendations regarding APP 10.

APP 11: Security of Personal Information

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 DIBP and AFP 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 the AFP 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.

Access control measures provided under the IDSA will mitigate misuse and unauthorised access, modification or disclosure, including by AFP employees. As noted in the section on training and management of FVS users, access to the FVS will only be provided to a limited number of nominated users from the AFP, restricted to employees who have a reasonable need to use the FVS to fulfil their employment functions. In accordance with the FVS Access Policy, the AFP will be required to maintain a register of nominated users for oversight and auditing purposes. Audits will be undertaken annually and will examine records that identify the time, purpose and nominated user associated with each

transaction. These records will provide the ability to detect any anomalous or potentially suspicious transactions. These oversight measures will provide a strong deterrent for misuse of personal information by AFP users.

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

APP 12: Access to Personal Information

There is no Personal Information retained in the FVS about individual members of the public who are the subject of transactions, only transaction IDs held in the audit logs that are meaningless outside the AFP (plus the usernames of the authorised users involved in the transactions). There is no Personal Information in the system at all to which a member of the public could, in principle, have a right to access.

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 AFP-DIBP use case covered in this Report 2 – should bring an important improvement to the privacy of biometric data processed by government agencies. Facial biometric data is a critical asset 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 facilitate, control and, where necessary, constrain the flow of facial data between government agencies.

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

- The FVS will, over time, reduce the exposure of biometric data, by helping DIBP and the AFP shift from *ad hoc* data transfers to more specific transactions.
- 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].

The flow of facial biometric data between DIBP and the AFP may not be reduced by the FVS *Retrieve* function alone. Unlike the DIBP-DFAT flows assessed in Report 1 in the present PIA series, there is not a significant bulk flow of Personal Information in question. The principle privacy benefit of the DIBP-AFP implementation of FVS *Retrieve* relates not to volume but to the improved control and consistency of one-off biometric data exchange.

Recommendations

For the operation of the initial, portal-based Face Verification Service being conducted between DIBP and the AFP 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 would recommend that a further privacy analysis be done on the system-to-system functionality, and their 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]. *Interoperability Hub Technical Concept of Operations*, Attorney-General's Department, October 2015
Filename: Technical Concept of Operations.docx
- [4]. *'Verification -> Retrieve' Function - DIBP Citizenship Data*, Attorney-General's Department, V0.6 12/02/16
Filename: Business Requirements - Retrieve Function - DIBP Citizenship Data - V0.5....docx
- [5]. *Face Matching Services*, (undated), Attorney-General's Department
Filename: Fact-Sheet-National-Facial-Biometric-Matching-Capability.pdf
- [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]. *Australian Federal Police Privacy Statement*
www.afp.gov.au/global/privacy
- [9]. *AFP Privacy Policy*
<http://www.afp.gov.au/~media/afp/pdf/a/afp-privacy-policy-001.pdf>
(accessed 11 April 2016)
- [10]. *Concept of Operations National Facial Biometric Matching Capability v0.7*
Filename: Concept of Operations - National Facial Biometric Matching Capability - .pdf
- [11]. *Blueprint National Facial Biometric Matching Capability* (undated),
Filename: Master Blueprint - National Facial Biometric Matching Capability - Nov 2...pdf

External References

- [12]. *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)*
- [13]. *Australian Federal Police Act 1979 (Cth)*
http://www.austlii.edu.au/au/legis/cth/consol_act/afpa1979225/

- [14]. *Citizenship Act 2007 (Cth)*
http://www.austlii.edu.au/au/legis/cth/consol_act/aca2007254/
- [15]. *Migration Act 1958 (Cth)*
http://www.austlii.edu.au/au/legis/cth/consol_act/ma1958118/
- [16]. *Australian Border Force Act 2015 (Cth)*
http://www.austlii.edu.au/au/legis/cth/num_act/abfa2015225/
- [17]. *Privacy notice form 1442i*, Department of Immigration and Border Protection
<https://www.border.gov.au/Forms/Documents/1442i.pdf>
- [18]. *Your personal identifying information form 1243i*, Department of Immigration and Border Protection
<https://www.border.gov.au/Forms/Documents/1243i.pdf>
- [19]. *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>
- [20]. *Martin Place Siege: Joint Commonwealth - New South Wales review*, Department of Prime Minister and Cabinet, and NSW Premier and Cabinet, January 2015
https://www.dpmmc.gov.au/sites/default/files/publications/170215_Martin_Place_Siege_Review_1.pdf
- [21]. *New \$18.5 million biometrics tool to put a face to crime*, Minister for Justice, Media Release, 9 Sept 2015
- [22]. *Document Verification Service Privacy Policy*
<http://www.dvs.gov.au/Pages/Disclaimers/Privacy-statement.aspx>
(accessed 14 Jan).