AFP
AUSTRALIAN FEDERAL POLICE

Privacy Impact Assessment

Pilot of Forensic/Investigative Genetic Genealogy

POLICING FOR A SAFER AUSTRALIA

Report title	Privacy Impact Assessment for Pilot of Forensic/Investigative Genetic Genealogy
Originating area	AFP Forensics
Date produced	22 February 2023
Classification	OFFICIAL
Cleared by	AFP Privacy Officer AFP Forensics
Prepared by	Maddocks Lawyers
Endorsed by	National Manager Forensics

Contents

Executive Summary

1. Forensic/Investigative Genetic Genealogy (**F/IGG**) is a forensic technique that uses deoxyribonucleic acid (**DNA**) analysis in combination with information available via public genetic and genealogy databases, to support investigation processes used to identify human remains and perpetrators of crime.

2. It was first used in the identification of human remains, but F/IGG came to prominence in 2018 in the highly publicised 'Golden State Killer' case in California, United States. The Golden State Killer was reported to have committed at least 12 murders and 45 sexual assaults in areas of California in the 1970s and 1980s. Investigators used traditional investigative methods to investigate the case in the decades that followed, but it was the use of online genealogy records which allowed investigators to narrow their focus to a handful of suspects, ultimately leading to the arrest, guilty plea and conviction of Joseph De Angelo.[1]

3. F/IGG has since been used to generate investigative leads in numerous countries, including the United States, Canada and a pilot in Sweden.

4. Short tandem repeat (**STR**) DNA analysis, which is currently used in criminal casework in Australia, only tests 21 sites or loci on an individual's DNA and can generally only detect close family relationships, such as parent-child and siblings. The F/IGG method uses DNA analysis techniques including whole genome arrays (**WGA**) or whole genome sequencing (**WGS**). WGA or WGS analysis analyses millions of Single Nucleotide Polymorphisms (SNPs) on an individual's DNA. The additional information available through the use of WGA or WGS analysis enables searching for extended familial relationships (fourth and fifth cousins, and beyond).

5. Once WGA or WGS analysis is complete and DNA data has been obtained from a biological sample, between 500,000 and 1,000,000 SNPs (each represented by a C,G,T or an A) is uploaded to a genealogy database to identify any familial links. As at the date of this PIA, only a very limited number of genealogy databases currently allow law enforcement agencies to upload DNA data for law enforcement purposes, including the United States based genealogy databases, GEDmatch PRO, FamilyTreeDNA and DNASolves (**Genetic Genealogy Databases**).

6. If a potential relative of the unknown DNA donor, who has uploaded their own genetic data for law enforcement matching as permitted under the site's terms and conditions, shares segments of identical DNA with the unknown donor, law enforcement can view this information (e.g. the amount of shared DNA between the two individuals, measured in centimorgans). Family trees are then constructed in an attempt to link the potential relative with the unknown DNA donor. This requires skill in genealogical techniques, and depending on the closeness of the relationship, may prove complex and time consuming.

[1] Nathan Scudder, Runa Daniel, Jennifer Raymond and Alison Sears, 'Operationalising forensic genetic genealogy in an Australian context' (2020) 316(110543), Forensic Science International.

7. The AFP, in collaboration with the New South Wales Police Force (**NSWPF**), Victoria Police and The Victorian Institute of Forensic Medicine, is undertaking a project (**Project**), including to assess the viability of F/IGG for operational implementation at a federal level by the AFP.

8. The aim of the Project for the AFP is for F/IGG to be implemented and used by the AFP to identify victim human remains and perpetrators of violent crime, when routine criminal investigative processes have been exhausted.[2]

9. The broad objectives of the Project include:

   9.1 to assess the scientific validity and robustness of the various platforms and service providers available to generate the DNA data required for F/IGG;

   9.2 to assess the genealogical search process, including assessment of sourcing external experts versus developing an internal capability, to determine whether the technique is relevant to Australian casework in the short and long term;

   9.3 to assess the legal and ethical climate in regard to F/IGG;

   9.4 to develop education packages and material for AFP investigators and stakeholders;

   9.5 if F/IGG is deemed viable, to develop an operational pathway to implementation, including appropriate policies, reporting and governance frameworks; and

   9.6 to progress a pilot case, involving a criminal investigation, for F/IGG to better inform internal process and guide consultation on a final PIA.

10. As the Project will involve the AFP handling a range of personal information, the AFP engaged Maddocks to prepare this Privacy Impact Assessment (**PIA**) to determine whether the AFP's implementation of the Project will comply with the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**[3]).

11. Undertaking a PIA is consistent with the requirements of the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (**APP Code**), which has applied from 1 July 2018. The APP Code requires agencies to undertake a written PIA for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information, but undertaking a PIA also reflects privacy 'best practice' for other projects.

[2] F/IGG can also be used to identify human remains where the individual is not suspected of being the victim of a crime, but this use is the subject of separate privacy impact assessment processes, and is out of scope for this PIA process.

[3] Maddocks has conducted its analysis on the basis that the factual information provided by the AFP, as set out in the Project Description of this PIA report) is up-to-date, complete and correct. Additionally, Maddocks' analysis in this PIA reflects the provisions of the Privacy Act, and associated case law and guidance material, as at the date of analysis on page 2 of this PIA report. Finally, this PIA:

- does not analyse or examine any information flows, or associated privacy risks or compliance issues, that are not described in the Project Description of this PIA Report; and
- has been conducted from the perspective of the AFP, and not any other entity.

12. This PIA:

12.1 considers compliance with the Privacy Act, including the APPs, in the context of the AFP's implementation of the Project;

12.2 sets out the information flows, which helps to highlight privacy risks and areas for improvement in terms of risk mitigation;

12.3 is intended to help the AFP manage identified privacy risks and impacts, in respect of its implementation of the Project;

12.4 may serve to inform the AFP and other stakeholders about the privacy elements of the AFP's implementation of the Project; and

12.5 considers the safeguards that have been, or should be, put in place to secure personal information from misuse, interference or loss, or from unauthorised access, modification or disclosure.

13. This PIA builds upon the extensive work done by the NSWPF in respect of its implementation of F/IGG, noting that the NSWPF, Victoria Police, The Victorian Institute of Forensic Medicine and the AFP have conducted extensive stakeholder consultation as part of assessing the viability of F/IGG for operational implementation in NSW. A summary of these consultation processes is set out at **Appendix D – Summary of stakeholder consultation**. The AFP's intention is to consult with further Commonwealth stakeholders (including the Office of the Australian Information Commissioner (**OAIC**)) as the project progresses into an enduring capability.

Recommendations

14. **Recommendation 1:**

Adopt a transparent and open approach to the Project, including by:

- broadly consulting with experts in the F/IGG and privacy fields;
- publishing this PIA and other associated details of the Project (or an appropriate summary of its findings and recommendations); and
- openly describing the AFP's proposed use of F/IGG.

For example, developing a dedicated webpage that explains how the AFP will use F/IGG. Additionally, publicising the use of F/IGG, including publishing statistics on successful and unsuccessful use of F/IGG.[4]

[4] Acknowledging that publishing this data may need to be delayed for operational security reasons or while matters are before the court, particularly when the number of occasions when F/IGG has been attempted by the AFP is very small.

15. **Recommendation 2:**

As there is no Commonwealth legislation that covers the use of F/IGG at a federal level, ensure any internal policies, standard operating procedures and governance structures to guide the use of F/IGG are reviewed by relevant stakeholders so they are robust and stringent enough to reassure key stakeholders (and by extension, the general public) that in using F/IGG, the AFP is appropriately balancing the competing interests of public safety and individual privacy. As such, ensure internal policies, standard operating procedures and governance structures are regularly reviewed and updated with input from relevant stakeholders (as required).

Develop, implement and maintain internal policies, standard operating procedures and governance structures to guide its use of F/IGG, including the circumstances in which the technique may be used, for example to include that:

- F/IGG will only be used in the course of an active criminal investigation to assist the AFP to identify human remains to identify perpetrators where it is likely that a serious crime (e.g. murder or sexual assault) has been committed;

- F/IGG will only be used in the course of an active criminal investigation when a senior officer/s has made a determination that, in all the circumstances:
    - other less privacy-intrusive investigative and forensic processes have been exhausted; or
    - there is a significant and immediate threat to public safety or the safety of individuals,

  and the identity of the human remains or perpetrator is unknown; and

- F/IGG will only be used in accordance with the AFP's standard investigative and law enforcement procedures.

Finally, document how the AFP will conduct case reviews to determine when DNA Data should be removed from, or re-uploaded to, Genetic Genealogy Databases. The document should provide clear guidance that explains how the AFP will balance the privacy risks associated with the Genetic Genealogy Database holding the DNA Data (e.g. increased security risks) against the likelihood of the DNA Data being matched on the relevant database.

16. **Recommendation 3**

Ensure:

- contractual arrangements or terms of service with any third party laboratory, third party company or contractor or Genetic Genealogy Database contain appropriate security and privacy protections, including an obligation to:

    - only use and disclose information collected as part of the Project for the purposes of delivering services to the AFP under the contract;

    - take all reasonable steps to ensure that information collected as part of the Project is protected from misuse, interference and loss, and from unauthorised access, modification or disclosure;

- delete all information collected as part of the Project when directed to do so by the AFP;

- extracted DNA samples that are sent by courier to a private third party are appropriately protected in transit;

- the secure platform via which the third party laboratory will transfer DNA Data to the AFP is suitably secure;

- the secure cloud storage platform via which it will disclose DNA Data to, and receive DNA Data from, the third party company or contractor is suitably secure; and

- its method of transmission of DNA Data to, and Familial Link Data from, the Genetic Genealogy Databases is suitably secure.

Scope of PIA

17. This PIA only analyses the information flows, and associated privacy risks or compliance issues, that are described in the Project description of this PIA Report.

PIA methodology

18. This PIA has been prepared by Maddocks and conducted in accordance with the following methodology, which is consistent with the *Guide to undertaking privacy impact assessments* (**PIA Guide**) issued by the OAIC.

Stage	Description of steps
1.	**Plan for the PIA:** Maddocks reviewed relevant background material provided by the AFP (listed in **Appendix D – Material Reviewed**), and were provided a briefing by officers from AFP. It was agreed that the AFP template PIA would be used to prepare a report of the PIA, and that Maddocks would use the extensive formal stakeholder consultation process that had been undertaken in connection with a PIA conducted in respect of NSWPF's use of FIGG technology (please refer to **Appendix B – Summary of stakeholder consultation**). Given this, it was agreed that additional consultation processes with additional individuals or groups that might be impacted by the issued raised in this PIA was not required. In addition, when undertaking the analysis and forming views about risks, Maddocks also took into account its previous experience and research about reasonable community expectations of privacy. For example, the *Australian Community Attitudes to Privacy Survey 2020* commissioned by the OAIC contains useful information regarding current community expectations, including about the level of trust in government agencies' handling of personal information.

Stage	Description of steps
2.	**Project description**: Maddocks prepared an initial draft Project description, including drawing upon the description of the relevant technology in a previous PIA conducted by the NSWPF, which described the Project. This draft was refined and then finalised following feedback from AFP.
3.	**Privacy impact analysis and compliance check:** In this step Maddocks focussed on compliance against each relevant APP and privacy best practice. In undertaking its analysis, Maddocks considered and applied the *Australian Privacy Principles guidelines* (**APP Guidelines**) issued by the OAIC, which outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters that may be taken into account when assessing the AFP's compliance with the Privacy Act.
4.	**Privacy management and addressing risks:** Maddocks considered potential mitigation strategies that could reduce or remove the privacy impacts and risks identified during the previous step, and developed recommendations.
5.	**Draft report:** Maddocks prepared a draft version of this PIA report.
6.	**[Further refinement of draft PIA report**: Following review of the draft report by the AFP, Maddocks further refined the analysis and potential mitigation strategies as required to ensure that privacy risks were appropriately considered and addressed.
7.	**Final Report**: Maddocks finalised this PIA report.

19. Maddocks has also consulted with the Project team and AFP Legal in the preparation of this PIA. In addition to written and verbal instructions provided by the Project team and AFP Legal, the following legislation, policies and documents are relevant to this PIA:

19.1 the Privacy Act;

19.2 the *Australian Federal Police Act 1979* (Cth);

19.3 Australian Government Protective Security Policy Framework;

19.4 AFP Privacy Policy;

19.5 AFP Information Management Handbook (MIDMA012);

19.6 AFP National Guideline on Information Management;

19.7 AFP National Guidelines in Information Security: ICT systems, hardware and software;

19.8 AFP National Guideline on Privacy;

19.9 *Privacy Threshold Assessment – Pilot use of Forensic/Investigative Genetic Genealogy for ACT cold case investigation*, dated November 2022; and

19.10 *New South Wales Police Force Privacy Impact Assessment*, dated 8 December 2022.

20. A glossary of defined terms and acronyms is at **Appendix C – Glossary** of this PIA report.

Project description

21. As discussed in the Executive Summary, the AFP, in collaboration with the NSWPF, Victoria Police and The Victorian Institute of Forensic Medicine, is undertaking the Project to assess the viability of F/IGG for operational implementation at a federal level by the AFP.

22. The key information flows and methodology for the Project are set out below.

Key information flows and Project methodology

23. The Project will involve the handling of information, including personal information, by the AFP. Due to the complex nature of the key information flows, there will be multiple collections of information, including personal information, by the AFP.

24. In summary, the key steps involved in the AFP's proposed use of F/IGG are as follows:

24.1 the AFP will collect a biological sample from unidentified human remains in the context of a criminal investigation or material left at a crime scene by an unidentified potential perpetrator (this step does not represent a change to existing investigative processes or procedures);

24.2 the biological sample will be processed by the AFP to extract a DNA sample (again, this step does not represent a change to existing investigative processes or procedures);

24.3 the extracted biological sample will be sent by the AFP to a private, third-party laboratory for DNA data (WGA or WGS) generation. The third party laboratory may be based interstate or overseas (including in the United States);

24.4 the DNA data (WGA or WGS) (**DNA Data**) will be returned to the AFP by the private, third-party laboratory and then sent by the AFP to a private, third party company or contractor for bioinformatics analysis to prepare the DNA Data for upload to a Genetic Genealogy Database. The third party company or contractor may be based in Australia or overseas (likely in the United States);

Note: the steps set out in paragraphs 24.3 and 24.4 may be combined if a third party laboratory can perform both the WGA or WGS DNA data generation and bioinformatics analysis.

24.5 Following the steps set out in paragraphs 24.3 and 24.4, DNA Data will be sent by the third party laboratory / third party company or contractor back to the AFP via a secure cloud storage platform and uploaded by the AFP to the AFP's secure server, with restricted access;

24.6 DNA Data will be uploaded by the AFP to the Genetic Genealogy Database. If, as a result of the DNA Data being uploaded to the Genetic Genealogy Database:

(a) no suitable familial links are generated: a case review will be conducted and a decision made regarding whether the DNA Data is removed from the Genetic Genealogy Database; or

(b) suitable familial links are generated: a list of familial link data (including personal information such as names, aliases, email addresses, addresses, dates of birth and family trees (where available) (**Familial Link Data**) will be retrieved by the AFP;

24.7 Familial Link Data will be stored by the AFP on a secure server with restricted access;

24.8 the AFP will commence genealogical searches using Familial Link Data. This may involve the AFP using Familial Link Data by matching it against other data (**Open Source Data**), including:

(a) online via the AFP's ICT network (using genealogical websites and social media);

(b) via government records requests (for example, against State or Territory based registries of births, deaths and marriages); and

(c) via searches of AFP and law enforcement records, where permitted by law;

24.9 results of genealogical searches will be uploaded by the AFP to the AFP's secure server with restricted access and used to build family trees (using software owned by, or licensed to, the AFP);

24.10 an intelligence report based on results of genealogical searches will be prepared by the AFP for AFP investigators. The intelligence report will be used by the AFP to assist in further investigations designed to identify unidentified human remains or an unidentified potential perpetrator;

24.11 if an individual is identified as a potential familial link to the unidentified human remains or unidentified potential perpetrator, the AFP may obtain a DNA sample (containing **Reference Testing Data**) from the individual; and

24.12 if required, a court report will be generated by the AFP (please refer to step 13 of the Detailed Description of Information Flows for further information).

Who is responsible for the Project?

25. The AFP is the agency with primary responsibility for delivery of the Project at a federal level. The AFP is an 'agency' for the purposes of the Privacy Act, including in relation to policing services for the Australian Capital Territory.[5]

[5] The AFP operates on the basis that it is not subject to ACT privacy laws. This PIA only addresses the AFP's obligations under the Privacy Act.

26. The relevant AFP team members responsible for delivering the Project (as at the date of analysis) include:

26.1 Dr Nathan Scudder (Coordinator Biometrics)

26.2 s 47E(c) (Forensic Biologist); and

26.3 s 47E(c) (Acting Team Leader, Forensic Intelligence).

Information flows

27. Set out below is a summary description of the information flows associated with the Project, followed by a detailed description of the relevant information flows.

Summary Description of Information Flows

Issue	Summary
What information will be collected?	As discussed below, the information collected as part of the Project can be divided into the following categories: ▪ DNA Data; ▪ Familial Link Data; ▪ Open Source Data, and ▪ Reference Testing Data.

Issue	Summary
How will the information be collected?	<u>DNA Data</u> DNA Data will be collected as follows: ▪ a biological sample will be collected from unidentified human remains or an unidentified potential perpetrator by the AFP in the context of a criminal investigation; ▪ a DNA sample extracted from the biological sample will be collected by the AFP; ▪ DNA Data will be collected from a private, third party laboratory by the AFP; and ▪ enhanced DNA Data will be collected from a private, third party company or contractor. **Note: the third and fourth dot points may be combined if a third party laboratory can perform both the WGA or WGS DNA data generation and bioinformatics analysis.** <u>Familial Link Data</u> Familial Link Data will be collected from Genetic Genealogy Databases by the AFP. <u>Open Source Data</u> Open Source Data will be collected from various sources (including online via the AFP networking (using genealogy websites and social media), via government record requests (via State and Territory Registries of Births, Deaths & Marriages, etc.) and via searches of AFP records) by the AFP. Open Source Data will be collected lawfully, and in accordance with the AFP's existing policies and procedures[6]. <u>Reference Testing Data</u> Reference Testing Data (if any) will be collected directly from the relevant individual. DNA Data will be extracted from the Reference Testing Data.[7]

[6] The collection of Open Source Data is outside the scope of this PIA as it is a business as usual function of the AFP.
[7] The collection of Reference Testing Data is outside the scope of this PIA as it is a business as usual function of the AFP.

Issue	Summary
How will the information be stored?	Information collected as part of the Project will be held in an AFP server at a secure location and protected against unauthorised access. Information collected as part of individual investigations will be held in specific case files with restricted access on a case by case basis. The AFP maintains 'state of the art' data security systems, to protect the security, privacy, confidentiality and integrity of the data it holds. As detailed below, access to specific case files will be restricted using network or system authentication including a username and password, and will be subject to audit logging. On completion of the relevant operation or investigation, all stored information will be archived on the AFP's records management system in accordance with AFP policy, with restricted access and retention in accordance with the *Archives Act 1988* (Cth).

Issue	Summary
Who will have access to the information?	Third parties will have access to information as follows: ▪ A private, third party laboratory will have access to a DNA sample in order to undertake WGA or WGS DNA Data generation. Following generation of the DNA Data, if any of the DNA sample remains, it will be returned to the AFP or destroyed by the third party laboratory. ▪ A private, third party company or contractor will have access to DNA Data in order to perform bioinformatics analysis to prepare the DNA Data for upload to Genetic Genealogy Databases. Following completion of the bioinformatics analysis, the DNA Data will be permanently deleted by the third party company or contractor. ▪ Genetic Genealogy Databases will have access to the DNA Data when the DNA Data is uploaded to the relevant database by the AFP. o If no suitable familial links are generated, the DNA Data may be removed from the Genetic Genealogy Databases or retained for an agreed period of time (following a case review process). If removed, it may be re-uploaded by the AFP after an agreed timeframe, to see if any additional suitable familial links are generated. o If suitable familial links are generated, the DNA Data is removed from the Genetic Genealogy Databases after initial casework is complete. ▪ Third party genealogists (if required) may have access to Familial Link Data and Open Source Data in order to assist the AFP to build family trees. Any such third party genealogists will be contracted by the AFP, subject to security vetting and will only work within the AFP's secure environment. Within the AFP, access to the information will be restricted to only those authorised personnel who require access to perform their duties (i.e. a user involved with a specific operation or investigation) or authorised third party genealogists (if required). Those individuals will be required to identify themselves using a unique username and password to access the information. Access to the information will also be subject to audit logging and staff will be held accountable for any misuse of the technology.

What will the information be used for?

The information will be used by the AFP to perform its operational duties in the identification of human remains in the context of a criminal investigation, the investigation of crime and protection of the community.

Specifically, the following types of information will be used for the following purposes:

- **Biological sample:** A biological sample will be used for the purpose of extracting a DNA sample.
- **DNA sample:** A DNA sample extracted from a biological sample will be used by a private, third party laboratory to generate additional DNA Data required for F/IGG.
- **DNA Data:** DNA Data will be used by a bioinformatician to process the DNA Data to collate the required DNA markers so the DNA Data is in a form that can be compared to DNA Data uploaded by individuals to the Genetic Genealogy Databases.
- **Processed DNA Data:** Processed DNA Data, generally comprising of between 500,000-1,000,000 SNPs, will be used to upload to the genetic Genealogy Databases for the purposes of identifying potential familial links.
- **Familial Link Data:** Familial Link Data will be used to build family trees that may lead to common ancestors, which can then provide intelligence as to the identity of the unknown victim human remains or potential perpetrator. Any names/aliases, email addresses, nominated genders and family trees (if available) are used to firstly identify who these individuals are. Once known, the individual's family tree will be built to try and identify common ancestors between the links. These groups of linked individuals can then provide direction as to where in the family tree the unknown individual is likely to be placed. These lines will be built down to the present day (or relevant time period) to indicate candidates for the unknown individual based on the circumstances of the particular case.
- **Open Source Data:** Open Source Data (such as information collected from social media, public websites and genealogical databases and public records) is used to identify any potential familial links, and to assist in the development of family trees.
- **Reference Testing Data:** Reference Testing Data (including DNA Data included within such Reference Testing Data) will be used to either eliminate certain branches of a family tree or identify which branches of a family tree the AFP should investigate to ascertain the identity of victim human remains or a potential perpetrator of a serious crime.

Personal Information will only be collected, used and retained for law enforcement purposes, in line with relevant legislation and principles including the *Crimes Act 1914* (Cth), *Australian Federal Police Act 1979*

Issue	Summary
	(Cth) and Privacy Act. Court ordered destruction will also apply in relation to the information.
Are there third parties to whom it will be routinely or otherwise disclosed?	The AFP will disclose the DNA sample to a private, third party laboratory for WGA or WGS Data generation. The third party laboratory may be based interstate or overseas (including in the United States). The AFP will arrange a courier to transport the physical DNA extract to the relevant third party laboratory. The AFP will disclose the DNA Data to a private, third party company or contractor for bioinformatics analysis. The third party may be based interstate or overseas (likely in the United States). The AFP will disclose the DNA Data to the third party via secure file transfer using a secure cloud storage platform. The AFP will upload (and therefore disclose) the DNA Data to the Genetic Genealogy Databases to determine if there are any familial links between the DNA Data and the DNA Data uploaded to the Genetic Genealogy Databases by customers of the Genetic Genealogy Databases who, for criminal investigations, will each have consented to the use of their DNA Data and Familial Link Data for law enforcement purposes. Where required, the AFP may also disclose information to a third party, contracted and security vetted genetic genealogist. The AFP does not intend to 'routinely' share this information with any external agencies or any third parties (other than those listed above). Information may be shared for operational purposes, such as the protection of individuals or for public safety, where authorised or as required by law including under the *Crimes Act 1914* (Cth), *Australian Federal Police Act 1979* (Cth) and Privacy Act.

Detailed Description of Information Flows

Step	Summary	Data type
1	The AFP collects a biological sample from unidentified human remains where the individual is suspected to be the victim of a crime[8]. OR The AFP collects a biological sample from an unidentified potential perpetrator of a crime.[9] [10]	Biological sample
2	The biological sample is processed to extract a DNA sample.	DNA sample
3	The AFP sends the extracted DNA sample via courier to a private, third party laboratory for WGA or WGS DNA data generation. The third party laboratory may be based interstate or overseas (including in the United States).	DNA sample
4	The third party laboratory undertakes WGA or WGS DNA data generation and the DNA Data is transferred by the third party to the AFP, via a secure platform. The DNA Data will be uploaded by the AFP to the AFP's secure server, with restricted access.	DNA Data
5	The AFP provides the DNA Data via a secure cloud storage platform to a private, third party company or contractor for bioinformatics analysis in order to prepare the DNA Data for upload to a Genetic Genealogy Database. The third party may be based interstate or overseas (likely in the United States). **Note: Steps 4 to 7 may be combined if a third party laboratory can perform both the WGA or WGS DNA data generation and bioinformatics analysis.**	DNA Data

[8] In the NSWPF PIA, this is described as 'Scenario 2'.
[9] In the NSWPF PIA, this is described as 'Scenario 3'.
[10] As discussed in Footnote 2, F/IGG can also be used where a biological sample is collected from unidentified human remains where the individual is not suspected to be the victim of a crime (in the NSWPF PIA, this is described as 'Scenario 1'). However, as this is out of scope, this PIA does not specifically analyse the information flows associated with this scenario against the APPs.

Step	Summary	Data type
6	The third party company or contractor undertakes bioinformatics analysis and the processed DNA Data is transferred by the third party to the AFP, via a secure cloud storage platform. The amended DNA Data will be uploaded by the AFP to the AFP's secure server, in a specific case file with restricted access. Once bioinformatics analysis has been performed and the amended DNA Data provided to the AFP, any remaining DNA Data will be permanently deleted by the third party company or contractor.	DNA Data
7	The AFP uploads the DNA Data to a Genetic Genealogy Database. If, as a result of the DNA Data being uploaded to a Genetic Genealogy Database: ▪ **No suitable familial links are generated**[11]: a case review is conducted and a decision made regarding whether the DNA Data is removed from the Genetic Genealogy Database or retained for an agreed period (but may be re-uploaded after an agreed timeframe to see if any suitable familial links are generated).[12] ▪ **Suitable familial links are generated**: a list of the Familial Link Data (including Personal Information such as names, aliases, email addresses, addresses, dates of birth and family trees (where available)) is retrieved by the AFP.	DNA Data / Familial Link Data
8	If suitable familial links are generated, the AFP will download the Familial Link Data to the AFP's secure server, in the secure network drive in a specific case file with restricted access	Familial Link Data

[11] Whether a familial link is 'suitable' is a subjective assessment, as it relies on a combination of the closeness of the familial link, the ability to identify the linked individual, and the availability of records to generate family trees to identify the connection between the link and the unknown. There is currently no defined threshold for 'suitability' of links resulting from Genetic Genealogy Databases.

[12] Considerations as to whether DNA Data is retained could include whether the DNA Data was derived from unidentified human remains (which weighs more heavily in favour of that individual's right to have their identity restored) or, if from a suspect, the likelihood of that individual committing a further serious offence during the period when the DNA Data was not uploaded and any new Familial Links not available to the AFP.

Step	Summary	Data type
9	The AFP commences genealogical searches using Familial Link Data. Genealogical searches involve the AFP using Familial Link Data to match Familial Link Data: ▪ online via the AFP network (using genealogy websites and social media; ▪ via government record requests (via State and Territory Registries of Births, Deaths & Marriages, etc.); and ▪ via searches of AFP and law enforcement records, as permitted by law, in accordance with AFP policies and procedures. The genealogical searches will be undertaken by AFP staff. External professional genetic genealogists may be contracted by the AFP to provide mentoring and assistance with difficult searches, where required. Such contractors will undertake AFP security vetting prior to engagement and will be given access to AFP systems, so all records will remain on secure AFP servers.	Familial Link Data / Open Source Data
10	The AFP will upload results of genealogical searches to the AFP's secure server, in a specific case file with restricted access and will use the results of the genealogical searches to build family trees (using software owned by, or licensed by, the AFP).	Familial Link Data / Open Source Data
11	The AFP will produce an intelligence report based on results of genealogical searches and family tree building for AFP investigators. The intelligence report will be used by the AFP to assist to identify unidentified human remains or an unidentified potential perpetrator (in accordance with normal operational and criminal investigative processes, using the information contained in the intelligence report as an investigative lead).	Familial Link Data / Open Source Data
12	**Optional step:** If an individual is identified as a potential familial link to the unidentified human remains or unidentified potential perpetrator, the AFP may obtain a DNA sample (containing **Reference Testing Data**) from the individual with that person's informed consent	Reference Testing Data
13	A court report is generated by the AFP (if required). It is anticipated that F/IGG will rarely be used within a court setting given that the standard STR DNA profile will be used to confirm the identity of the unidentified individual. This means that the results of F/IGG analysis will not have any evidentiary weight, but will be used as an investigative lead.	Familial Link Data / Open Source Data / Reference Testing Data

Analysis

28. As a preliminary matter, it is important to consider whether DNA Data, Familial Link Data, Open Source Data and Reference Testing Data is 'personal information' for the purposes of the Privacy Act.

29. The Privacy Act contains the following definitions:

    29.1 section 6(1) of the Privacy Act defines sensitive information as including *'genetic information about an individual that is not otherwise health information'*; and

    29.2 section 6FA(d) of the Privacy Act defines health information as including *'genetic information* about *an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual'.*

30. DNA Data, Familial Link Data and Reference Testing Data is therefore 'sensitive information' for the purposes of the Privacy Act. Open Source Data may also be 'sensitive information' as it may include genetic information.

31. On this basis, this PIA report treats all DNA Data, Familial Link Data, Open Source Data and Reference Testing Data as 'sensitive information' for the purpose of the Privacy Act.

32. As a further preliminary matter, the personal information of deceased persons is not protected by the Privacy Act[13]. Nevertheless, it is apparent from stakeholder consultation and relevant research (including that mentioned in the 'Methodology' section of this PIA Report) that the Australian community is likely to still consider it important to protect the personal information of deceased persons, particularly in circumstances where information about a deceased person could also constitute personal information about a living person.

33. For example, paragraph B.99 of the APP Guidelines states:

> *'Information about a deceased person may include information about a living individual and be 'personal information' for the purposes of the Privacy Act. For example, information that a deceased person had an inheritable medical condition may indicate that the deceased person's descendants have an increased risk of that condition. If the descendants are identifiable, that information would be personal information about the descendants. The privacy interests of family members could therefore be considered when handling information about deceased persons.'*

34. On this basis, this PIA Report treats personal information about deceased persons as 'personal information' for the purposes of the Privacy Act, unless expressly noted otherwise.

[13] However, some jurisdictions (e.g. the NSW and the ACT) do afford privacy protections to the personal information of deceased individuals, subject to some exemptions.

35. A detailed analysis of the Project against each of the APPs is set out in **Appendix A – Privacy assessment**.

Conclusion

If the recommendations identified above are implemented, it would be reasonable for the AFP to conclude that it has implemented sufficient checks and balances to protect individuals' privacy as part of the Project.

Appendices

This PIA report includes:

- Appendix A – Privacy Assessment
- Appendix B – Summary of stakeholder consultation
- Appendix C – Glossary

Appendix A – Privacy assessment

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION

APP 1.2 – Compliance with the APPs Have reasonable steps been taken to implement practices, procedures and systems relating to the AFP'S functions or activities to: — ensure compliance with the APPs? — enable inquiries or complaints about compliance with the APPs?	APP 1 is intended to ensure that entities manage personal information in an open and transparent way. Implementation of APP 1, including the adoption of an APP privacy policy (**Privacy Policy**), is the responsibility of the AFP. Undertaking PIAs such as this one supports the conclusion that the AFP is taking reasonable steps to implement practices, procedures and systems to comply with the APPs, as required under APP 1.2(a), and the APP Code. However, the AFP could take further steps to ensure that there is transparency regarding the Project (i.e. regarding the implementation of F/IGG by the AFP). This is particularly important in circumstances where stakeholders have raised significant privacy and ethical concerns regarding the use of F/IGG (please refer to **Appendix B – Summary of stakeholder consultation**). Please refer to **Recommendation 1**.	**Recommendation 1:** Adopt a transparent and open approach to the Project, including by: • broadly consulting with experts in the F/IGG and privacy fields; • publishing this PIA and other associated details of the Project (or an appropriate summary of its findings and recommendations); and • openly describing the AFP's proposed use of F/IGG. For example, developing a dedicated webpage that explains how the AFP will use F/IGG. Additionally, publicising

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
		its use of F/IGG, including publishing statistics on successful and unsuccessful use of F/IGG.
APP 1.3 to 1.6 – APP Privacy Policy Does the AFP have a clearly expressed and up-to-date policy about its management of personal information?	The AFP has developed a clearly expressed and up-to-date Privacy Policy detailing how it handles personal information. Each of the matters specified in APP 1.4 is addressed in the Privacy Policy which is available on the AFP's website. Relevantly for the purposes of the Project, the Privacy Policy reflects that: • the AFP collects, holds, uses and discloses personal information for purposes which are necessary for, or directly related to, the AFP's functions or	N/A
— Does it contain the information specified in APP 1.4?		

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
— Is it available free of charge and in an appropriate form?	activities as set out in section 8 of the *Australian Federal Police Act 1979* (Cth) and the Ministerial Direction; • the AFP collects a range of personal information, including: o *'records that assist in the enforcement of the criminal law, preservation of peace, the prevention, detection and investigation of criminal incidents, the protection of life, safety and property'*; and o *'investigation records'*; • the AFP may collect personal information from a third party or a publicly accessible source; and • the AFP uses and discloses personal information for the purposes for which it was collected, for purposes permitted by legislation and/or for purposes which are directly related to the AFP's functions. In Maddocks' view, the Privacy Policy is sufficiently broad as to cover the collections, uses and disclosures of personal information as part of the Project.	

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
APP 2 – Anonymity and pseudonymity Do individuals have the option of not identifying themselves, or using a pseudonym? If not, does an exception in APP 2.2 apply?	APP 2.1 requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym, when dealing with the entity in relation to a particular matter, unless an exception in APP 2.2 applies. Relevantly, APP 2.2(b) provides that an APP entity may deal with identified individuals if it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym. In Maddocks' view, given the proposed use of the Project in relation to law enforcement matters, it would clearly be impracticable for the AFP to deal with individuals who have not identified themselves or who have used a pseudonym. Maddocks therefore considers that the AFP will comply with APP 2.1 by virtue of the exception in APP 2.2(b).	N/A

APP 3.1 – Collection of solicited personal information Does the collection of solicited personal information directly relate to, or is it reasonably necessary for, an AFP function?	The AFP will collect: • biological samples from unidentified human remains where the individual is suspected to be the victim of a crime; • biological samples from an unidentified potential perpetrator of a crime; • DNA Data from a third party laboratory undertaking WGA or WGS DNA Data generation; • enhanced DNA Data from a third party company or contractor responsible for undertaking bioinformatics analysis; and • Familial Link Data from Genetic Genealogy Databases. This information will be 'solicited' by the AFP, noting that APP 3 only applies to 'solicited information. An agency (like the AFP) can only collect solicited personal information if it is reasonably necessary for, or directly related to, one or more of the agency's functions or activities. This is a two-step process that involves identifying the agency's functions or activities, and determining whether the collection is reasonably necessary for or directly related to those function or activities. Relevantly, the AFP's functions and activities include a range of law enforcement activities, as set out in section 8 of the *Australian Federal Police Act 1979* (Cth). In Maddocks' view, it is clear that the AFP's collection of biological samples, DNA Data and Familial Link Data will comply with APP 3 as the collection of such	**Recommendation 2**: As there is no Commonwealth legislation that explicitly covers the use by the AFP of F/IGG at a federal level (including for policing services in the Australian Capital Territory), ensure any internal policies, standard operating procedures and governance structures to guide the use of F/IGG should be reviewed by relevant stakeholders to ensure that they are robust and stringent enough to reassure key stakeholders (and by extension, the general public) that in using F/IGG, the AFP is appropriately balancing the competing interests of public safety and individual privacy. As such, internal policies, standard operating procedures and governance structures are regularly reviewed and updated by the

	information will be reasonably necessary for the AFP to undertake its law enforcement activities. Although Maddocks' considers that the AFP's collection of the relevant information will comply with APP 3, it nevertheless considers that the Australian community would expect that F/IGG would only be used in extenuating circumstances, given the potential privacy impacts associated with the use of F/IGG. For example, as discussed in **Appendix B – Summary of stakeholder consultation**, stakeholders have raised a number of privacy concerns, including about the fact that DNA sequencing could reveal health information and biogeographical information, the security of personal information in relation to building family trees, and the possibility of 'scope creep' in the use of F/IGG. Please refer to **Recommendation 2**. For completeness, we note that the 'data minimisation principle' requires an entity to only collect the minimum amount of personal information necessary to undertake its functions and activities. It is true that the AFP will need to collect personal information about a broad range of individuals to conduct F/IGG analysis, and as the analysis proceeds, it may become apparent that some of those individuals are not relevant to the investigation and therefore it may not be necessary to continue using their personal information for that investigation. However, the AFP will not know whether an individual is relevant to the investigation at the time of collecting the personal information. The AFP will therefore reasonably require information about these individuals in order to determine viable avenues of inquiry for the investigation.	AFP with input from relevant stakeholders (as required). Develop, implement and maintain internal policies, standard operating procedures and governance structures to guide its use of F/IGG, including the circumstances in which the technique may be used, for example to include that: • F/IGG will only be used in the course of an active criminal investigation to assist the AFP to identify human remains to identify perpetrators where it is likely that a serious crime (e.g. murder or sexual assault) has been committed; • F/IGG will only be used in the course of an active criminal investigation when a senior officer/s

		has made a determination that, in all the circumstances: ▪ other less privacy-intrusive investigative and forensic processes have been exhausted; or ▪ there is a significant and immediate threat to public safety or the safety of individuals, and the identity of the human remains or perpetrator is unknown; and • F/IGG will only be used in accordance with the AFP's standard investigative and law enforcement procedures.

APP 3.3 and 3.4 — Sensitive Information Is solicited sensitive information about an individual only collected with their consent? Is the collection reasonably necessary for, or directly related to the performance of that function?	APP 3.3 provides that an agency must not collect sensitive information about an individual unless: • the individual consents to the collection of the information, and the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or • an exception under APP 3.4 applies. It is important to recognise that if a consent-based model is not implemented, it is important that the AFP is only collecting personal information if it is certain that an exception under APP 3.4 applies to the particular information. Relevantly, APP 3.4(d) provides that sensitive information may be collected without consent if the APP entity is an enforcement body and it reasonably believes that the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. Given that the AFP is an enforcement body, and the collection of the biological samples, DNA Data and Familial Link Data is reasonably necessary for the AFP's functions and activities (refer to the discussion above regarding the application of APP 3.1), the AFP's collection of the biological samples, DNA Data and Familial Link Data will comply with APP 3.3 by virtue of the exception in APP 3.4(d). For completeness, any customers of a Genetic Genealogy Database will have consented to the collection (and use) of their DNA Data and Familial Link Data for law enforcement purposes. Although obtaining consent is a privacy-enhancing feature, the AFP does not have any visibility of the scope of these consents, or the mechanisms used to obtain them. In addition, any such consents are limited to the individual who uploaded their genetic information to the Genetic Genealogy Database, and other individuals listed in family trees may not have provided any	N/A

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
	consent. Accordingly, it is appropriate that the AFP is not relying on a consent-based model to implement the Project.	
APP 3.5 — Fair and lawful collection Are the means by which personal information will be collected lawful and fair?	A collection of personal information is lawful if it is not contrary to law. No law, legal order or legal principles will prevent the AFP from collecting the biological samples, DNA Data and Familial Link Data. Therefore, the collection will be by "lawful means". A "fair means" of collecting personal information is one that is not oppressive, does not involve intimidation or deception, and is not unreasonably intrusive. Whether a collection uses unfair means would depend on the circumstances. In Maddocks' view, the collection of the biological samples, DNA Data and Familial Link Data will be by fair means.	N/A
APP 3.6 – Collection from the individual Is personal information only collected from the individual?	APP 3.6 provides that the AFP must collect personal information about an individual only from the individual unless one of the exceptions apply. The AFP will collect biological samples directly from the individuals to whom they relate, and will also collect Reference Testing Data directly from the relevant individual. However, the AFP will collect DNA Data from the third party laboratory that undertakes the WGA or WGS DNA data generation, and from the third party company or contractor responsible for undertaking bioinformatics analysis. The AFP will also collect Familial Link Data from the Genetic Genealogy Databases.	N/A

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
If not, does an exception in APP 3.6 apply?	Relevantly, APP 3.6(b) provides that an agency may collect personal information about an individual from someone other than the individual if would be unreasonable or impracticable to collect the information directly from the individual to whom it relates. It is clear that the collection of the DNA Data and Familial Link Data directly from the individual to whom it relates would be impracticable. The AFP's collection of the DNA Data and Familial Link Data will therefore comply with APP 3.6 by virtue of the exception in APP 3.6(b).	N/A
APP 4 — Dealing with unsolicited information Will unsolicited personal information be received? How will it be handled?	It is very unlikely that the AFP will receive unsolicited personal information as part of the Project. However, in the event that the AFP does received unsolicited personal information (e.g. information about a person that is not the subject of a request to a Genetic Genealogy Database), the AFP will need to follow its usual procedures to ensure compliance with APP 4.	N/A

APP 5 — Notice of collection of personal information Will individuals be provided with notice of the matters referred to in APP 5.2 at or before the AFP collects information about the individual?	APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps to notify the individual of certain matters (referred to as 'APP 5 matters'), or otherwise ensure that the individual is aware of those matters. This notification must occur at or before the time of collection, or as soon as practicable afterwards. Relevantly, the APP Guidelines acknowledge that it may be reasonable for an APP entity to not take any steps to provide a collection notice. For example, paragraph 5.7 of the APP Guidelines provides that it may not be reasonable for an APP entity to provide a collection notice if: • *'notification may pose a serious threat to the life, health or safety of an individual or pose a threat to public health or safety, for example, a law enforcement agency obtaining personal information from a confidential source for the purpose of an investigation'*; or • *'notification may jeopardise the purpose of collection or the integrity of the personal information collected and there is a clear public interest in the purpose of collection, for example, a law enforcement agency undertaking cover surveillance of an individual in connection with a criminal investigation'*. It is not necessary for the AFP to provide a collection notice in respect of the collection of personal information about deceased persons, as the personal information of such persons is not protected by the Privacy Act. In respect of living persons, not providing a collection notice can be justified on the basis that it would not be reasonable if the notification of the collection would jeopardise the purpose of the collection (i.e. the conduct of a criminal investigation	N/A

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
	or an investigation into the identity of human remains), particularly as it is clear that there is a public interest in this collection of information by the AFP. On this basis, the AFP does not need to take any steps to ensure compliance with APP 5.	

APP 6 — Use or disclosure of personal information Will the project use or disclose any personal information for a secondary purpose? If yes, is this with the individual's consent, or does an exception in APP 6.2 apply?	The AFP will: • **use** biological samples by processing them to extract DNA samples; • **use** biological samples by storing them; • **disclose** DNA samples to a private, third party laboratory for WGA or WGS DNA data generation; • **use** DNA samples by storing them; • **disclose** DNA Data to a private, third party company or contractor for bioinformatics analysis in order to prepare the DNA Data for upload to the Genetic Genealogy Databases; • **disclose** DNA Data to the Genetic Genealogy Databases; • **use** DNA Data by storing it; • **use** Familial Link Data to conduct genealogical searches; • **use** Familial Link Data to build family trees that may lead to common ancestors, to indicate candidates for the unknown individual based on the circumstances of the particular case; • **use** Familial Link Data and Open Source Data to produce an intelligence report based on results of genealogical searches and family tree building;	**Recommendation 2:** Document how the AFP will conduct case reviews to determine when DNA Data should be removed from, or re-uploaded to, Genetic Genealogy Databases. The document should provide clear guidance that explains how the AFP will balance the privacy risks associated with the Genetic Genealogy Database holding the DNA Data (e.g. increased security risks) against the likelihood of the DNA Data being matched on the relevant database.

	• **use** Familial Link Data and Open Source Data, in the form of an intelligence report, to assist to identify unidentified human remains where the individual is suspected to be the victim of a crime or an unidentified potential perpetrator (in accordance with normal operational and investigative processes, using the information contained in the intelligence report as an investigative lead); • **use** Familial Link Data by storing it; • **use** Open Source Data to identify potential familial links, and to assist in the development of family trees; • **use** Open Source Data by storing it; • **use** Reference Testing Data to eliminate certain branches of a family tree or identify which branches of a family tree the AFP should investigate to ascertain the identity of human remains where the individual is suspected to be the victim of a crime or a potential perpetrator of a serious crime; • **use** Reference Testing Data by storing it; and • **use** Familial Link Data, Open Source Data and Reference Testing Data to generate a court report. In Maddocks' view, all uses and disclosures by the AFP of biological samples, DNA Data, Familial Link Data, Open Source Data and Reference Testing Data will be for the	

	primary purpose of collection (i.e. to enable the AFP to conduct its law enforcement functions). In this case, the AFP will comply with APP 6. However, even if a narrower interpretation of the permitted purpose is preferred (e.g. if the primary purpose is defined as the purpose of conducting F/IGG analysis to identify a victim or perpetrator), and one or more of the above uses or disclosures was therefore considered to be for a secondary purpose (e.g. disclosure to a contractor to prepare the sample to enable this to occur), Maddocks considers that the uses and/or disclosures will comply with APP 6 by virtue of the exception in APP 6.2(e). APP 6.2(e) provides that personal information may be used or disclosed for a secondary purpose if the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body. As the F/IGG technology has been successfully used by enforcement bodies to assist with the resolution of investigations, any secondary use or disclosure of personal information as part of the F/IGG process is likely to satisfy the exemption in APP 6.2(e). This is particularly so in circumstances where F/IGG analysis will only be used for investigating serious crimes, if all routine investigative procedures have already been exhausted. Implementation of **Recommendation 1** will assist in ensuring that the AFP is taking steps to ensure it is only using and disclosing personal information for enforcement-related activities in reasonably necessary circumstances, as required by APP 6.2(e). However, the AFP should consider and document how it will conduct case reviews to determine when DNA Data should be removed from, or re-uploaded to, Genetic Genealogy Databases. This is particularly important in circumstances where there are	

	increased security risks associated with having the DNA Data stored on the Genetic Genealogy Databases. Consideration has also been given to whether the *Guidelines on data matching in Australian Government administration* (**Data Matching Guidelines**) (which are voluntary, but the OAIC considers represent best practice) will apply to the Project. Guideline 1.1 Data Matching Guidelines provides that the guidelines apply to a data matching program if: • the program includes the comparison of two or more data sets, and at least two of the data sets each contain information about more than 5000 individuals; and • the data sets were collected for different purposes; and • the purpose of the program is: o to select individuals for possible administrative action; or o to add information from one database to another for purposes which include taking administrative action in relation to the individuals concerned; or o to add information from one database to another with the intention of analysing the combined information to identify cases where further administrative action may be warranted; or	

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
	○ to permanently combine the databases which provided the data sets being matched by the data matching program. Despite the broad definition of 'administrative action', it is unlikely that Data Matching Guidelines will apply to the Project, because at no stage will two data sets of over 5000 individuals be compared, noting that the Project involves the comparison of two data sets, one comprising of a single individual and one comprising of more than 5000 individuals. However, the AFP may wish to confirm with the OAIC whether it considers that the Data Matching Guidelines will apply to the Project.	
Will the project involve the disclosure of any biometric information (APP 6.3)?	APP 6.3 will not apply to the AFP as the AFP is an enforcement body.	N/A
Will the AFP use or disclose for an enforcement related activity?	Please see above.	N/A

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
APP 7 – Direct marketing Will the project involve use of any personal information for direct marketing purpose?	APP 7 applies to "organisations" as defined in the Privacy Act (and "agencies" only in limited circumstances that do not apply to the AFP). Accordingly, this APP does not apply to the AFP. Additionally, if Recommendation 3 is implemented, no third party laboratory, third party company or contractor or Genetic Genealogy Database will be able to use or disclose personal information for direct marketing (they will only be able to use such information for the purposes of delivering services to the AFP under the relevant contract). This will ensure that personal information in connection with the Project is not used in a manner inconsistent with APP 7.	N/A

APP 8 – Cross-border disclosure of information Will the project involve disclosure of any personal information to an overseas recipient?	APP 8 requires entities to take particular steps if they intend on disclosing personal information to an overseas recipient. APP 8.1 provides that, unless an exception in APP 8.2 applies, an APP entity may not disclose personal information to an overseas recipient unless it has taken such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information. The AFP will disclose DNA samples to private, third party laboratories for WGA or WGS DNA data generation. These third party laboratories may be based overseas (including in the United States). The AFP will also disclose DNA Data to a private, third party company or contractor for bioinformatics analysis in order to prepare the DNA Data for upload to the Genetic Genealogy Databases. The third party may be based interstate or overseas (including in the United States). Finally, the AFP will disclose DNA Data to Genetic Genealogy Databases, including those which are based in the United States It is therefore necessary to consider whether these disclosures of DNA samples and DNA Data to overseas recipients will comply with APP 8. Ideally, the AFP's contracts with third parties (including the Genetic Genealogy Databases which store personal information outside of Australia) would oblige the third party to comply with the APPs (other than APP 1). However, reaching such an outcome is likely to be extremely difficult to achieve in practice. Similarly, it may be difficult for the AFP to form a view that those third parties are subject to laws or a binding scheme that have the effect of protecting personal information in a way that, overall, is at least substantially similar to the way in which the APPs protect personal information. This is because the AFP may not have	N/A

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
	visibility about the applicable jurisdiction(s) in which personal information is stored at a particular point in time. If the AFP is unable to contractually oblige overseas recipients to comply with APPs, the AFP may be able to require those recipients to comply with specific requirements that mean that the recipient must handle personal information in a manner which is consistent with the APPs (so that a failure to do so would be a breach of a contractual obligation). This is likely to assist the AFP in demonstrating that it has taken reasonable steps in the circumstances to ensure that the overseas recipients do not breach the APPs (other than APP 1). Please refer to **Recommendation 3**.	
APP 9 - Adoption, use or disclosure of government related identifiers Will the project involve the adoption, use or disclosure of government related identifiers?	As APP 9 applies to "organisations" as defined in the Privacy Act (and "agencies" only in limited circumstances that do not apply to the AFP), this APP is not applicable to the AFP. Additionally, it is unlikely that any third party laboratory, third party company or contractor or Genetic Genealogy Database will be required to use or disclose a government related identifier. If a third party will be required to use or disclose a government related identifier, it will be important for the AFP's contract with the third party to require the use or disclosure of the relevant identifier.	N/A

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
APP 10– Quality of personal information *APP 10.1 – collection* Will reasonable steps be taken to ensure the personal information collected is accurate, up-to-date and complete?	Genetic information is static and is therefore always accurate, up to date and complete. This means that it is unlikely that, other than ensuring the biological samples are taken in a scientifically correct manner, any steps can be taken to ensure the quality of biological samples and DNA Data. Additionally, in the unlikely event that a third party provides incorrect DNA Data or Familial Link Data, this is mitigated by the fact that the F/ICG process is simply an avenue of investigation – i.e. the AFP would endeavour to collect further evidence about whether the individual is relevant to the investigation.	N/A
APP 10.2 – use/disclosure Will reasonable steps be taken to ensure personal information that is used or disclosed is accurate, up-to-date, complete and relevant?	Genetic information is static and is therefore always accurate, up to date and complete. This means that there are no steps that can be taken to ensure the quality of biological samples, DNA Data and Reference Testing Data. Additionally, we understand that the AFP already has existing policies and procedures that govern the collection of Open Source Data. We assume that these policies and procedures extend to ensuring the quality of the Open Source Data. We do not think that there are further reasonable steps that the AFP could take to ensure the quality of biological samples, DNA Data and Reference Testing Data..	N/A

APP 11.1 – Security of personal information
Will adequate steps be taken to protect personal information collected as part of project from:
(a) misuse, interference and loss; and
(b) unauthorised access, modification or disclosure?
	APP 11.1 requires an APP entity to take such steps as are reasonable to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
	We understand that the AFP is satisfied that any biological samples, DNA samples, DNA Data, Familial Link Data, Open Source Data and Reference Testing Data it holds will be subject to appropriate protections.
	In particular, we consider that it is appropriate that:
	• the information collected as part of the Project will be held in a secure AFP server at a secure location, and will be protected against unauthorised access;
	• the information collected as part of individual investigations will be held in specific case files with restricted access on a case by case basis;
	• the AFP maintains 'state of the art' data security systems, to ensure the security, privacy, confidentiality and integrity of the data it holds;
	• access to specific case files will be restricted using network or system authentication, including a username and password;
	• access to specific case files will be subject to audit logging;
	• the laboratory and the company will be required to permanently delete any DNA Data once the bioinformatics analysis has been performed and the DNA Data has been provided to the AFP;
		Recommendation 3:
		Ensure:
		• contractual arrangements or terms of service with any third party laboratory, third party company or contractor or Genetic Genealogy Database contain appropriate security and privacy protections, including an obligation to:
		  • only use and disclose information collected as part of the Project for the purposes of delivering services to the AFP under the contract;
		  • take all reasonable steps to ensure that

	• and contracted genealogists that have access to Familial Link Data and Open Source Data to assist the AFP to build family trees will be contracted by the AFP, subject to security vetting and will only work within the AFP's secure environment. However, we consider that it would be reasonable for the AFP to ensure that: • appropriate steps are taken to ensure that the extracted DNA samples that are sent by courier to a private third party laboratory are appropriately protected in transit; • its contractual arrangements with any private third party laboratory contain appropriate security and privacy provisions; • it is satisfied that the secure platform via which the third party laboratory will transfer DNA Data to the AFP is suitably secure; • it is satisfied that the secure cloud storage platform via which it will disclose DNA Data to, and receive DNA Data from, the third party company or contractor is suitably secure; • its contractual arrangements with any third party company or contractor contains appropriate security and privacy provisions; • its contractual arrangements with Genetic Genealogy Databases contain appropriate security and privacy provisions; and	information collected as part of the Project is protected from misuse, interference and loss, and from unauthorised access, modification or disclosure; • delete all information collected as part of the Project when directed to do so by the AFP; • it is satisfied that: • extracted DNA samples that are sent by courier to a private third party are appropriately

	• it is satisfied that its method of transmission of DNA Data to, and Familial Link Data from, the Genetic Genealogy Databases is suitably secure. Please refer to **Recommendation 3**. APP 11.2 provides that if an APP entity holds personal information about an individual and the entity no longer needs the information, the entity must take such steps as are reasonable in the circumstances to destroy the information, or to ensure that the information is de-identified. We note that any personal information collected by the AFP will be contained in a Commonwealth record and, as such, the AFP is not required to comply with APP 11.2. However, we consider it positive that on completion of an operation or investigation, all stored information will be archived on the AFP's record management system in accordance with AFP policy, with restricted access and retention in accordance with the *Archives Act 1988* (Cth). We also understand that Court ordered destruction will apply in relation to any personal information collected as part of the Project. However, it is important to ensure that any third parties required to handle personal information are required to destroy or deidentify the information once it is no longer required. We therefore agree that it is appropriate for the laboratory and the company to be required to permanently delete any DNA Data once the bioinformatics analysis has been performed and the DNA Data has been provided to the AFP	protected in transit; • the secure platform via which the third party laboratory will transfer DNA Data to the AFP is suitably secure; • the secure cloud storage platform via which it will disclose DNA Data to, and receive DNA Data from, the third party company or contractor is suitably secure; and • its method of transmission of DNA Data to, and Familial Link Data

FOCUS QUESTIONS	ANALYSIS	RECOMMENDATION
		from, the Genetic Genealogy Databases is suitably secure.
APP 12 – Access to personal information Can an individual obtain access to their information held by the AFP?	Under APP 12, an APP entity is required to give an individual access to the personal information held by it unless particular exceptions apply (depending on whether the APP entity is an agency or organisation). We do not consider that the implementation of the Project will impact the AFP's normal processes for compliance with APP 12. We therefore do not consider that any further steps are required by the AFP.	N/A

APP 13 – Correction of personal information Can an individual request correction of their personal information held by the AFP?	APP 13 requires an APP entity holding personal information to take such steps as are reasonable in the circumstances to permit correction of that information, except in limited circumstances. We do not consider that the implementation of the Project will impact the AFP's normal processes for compliance with APP 13. We therefore do not consider that any further steps are required by the AFP.	**N/A**

Appendix B – Summary of stakeholder consultation

1. As part of assessing the viability of F/IGG for operational implementation in NSW, the NSWPF, Victoria Police, The Victorian Institute of Forensic Medicine and the Australian Federal Police have conducted extensive consultation with domestic and international F/IGG stakeholders.

2. For example, the parties have:

    a. Consulted with the International Society for Forensic Genetics and other international stakeholders to consider some of the privacy and ethical considerations around the use of F/IGG, and to obtain the perspective of international experts on key F/IGG considerations. The key issues discussed in these consultations included:

        i. DNA sample sequencing and uploading DNA samples to online platforms, including issues regarding:

            1. outsourcing DNA sample sequencing (as most operational laboratories in Europe, the United States and Australia are not set up for WGA or WGS analysis);

            2. data retention and data being held by laboratories and online platforms; and

            3. sequencing data from indigenous populations.

        ii. Genealogy process and records access, including issues regarding:

            1. challenges to evidence and requests by defence to produce information;

            2. the use of 'in-house' versus outsourced genealogists;

            3. the security of personal information in relation to building family trees; and

            4. access to public and non-public records.

        iii. Reference testing, including issues regarding:

            1. the extent and scope of reference testing for F/IGG;

            2. transparency with relatives as to the purpose of reference testing; and

            3. consent for reference testing and whether this can validly be obtained.

        iv. Reporting, including issues regarding:
        v. where intelligence from F/IGG is being provided by a professional genealogist or DNA expert, is there the potential to mislead investigators ('White coat syndrome');

        vi. how to maintain transparency about the F/IGG process, while also protecting genetic informants from unwanted attention or risks to their safety;

        vii. the potential for 'bad actors' in the F/IGG process, whether through nefarious use of the technology, or unscrupulous operators and means to mitigate this; and

viii. application of the European Convention on Human Rights to reporting on F/IGG results.

b. Consulted with the Australian New Zealand Policing Advisory Agency and National Institute of Forensic Science Australia New Zealand Biology Specialist Advisory Group, to consider some of the privacy and ethical considerations around the use of F/IGG, and to obtain the perspective of experts on key scientific F/IGG considerations. The key issues discussed in these consultations included:

   i. DNA analysis, including issues regarding DNA quality;

   ii. genetic genealogy databases, including issues regarding data upload requirements, access by law enforcement, costs of use and terms and conditions requirements;

   iii. genealogy, including issues regarding access to records, developing family trees and the level of skill required to develop family trees; and

   iv. legal and ethical issues, including legislative requirements, international legal considerations and ethics approvals.

c. Conducted privacy and ethics workshops with Australian legal experts, to consider some of the privacy and ethical considerations around the use of F/IGG and to obtain the perspective of Australian legal experts on key F/IGG considerations. The key issued discussed in these consultations included:

   i. ensuring that interests of all individuals involved in the F/IGG process are protected, as DNA sequencing could reveal health information and biogeographical information;

   ii. the balance of interests between public safety and individual privacy;

   iii. issues regarding the F/IGG process being limited by genetic databases and individuals' DNA data included within those genetic databases;

   iv. issues regarding the collection of DNA data from an individual who is not connected to the crime scene (i.e. an innocent bystander);

   v. data retention issues, including issues regarding third parties securely holding and destroying data;

   vi. consent issues regarding broader familial relationships;

   vii. issues regarding uploading personal information to commercial websites, including that commercial websites may change their terms and conditions (and therefore which data can be used for law enforcement purposes) on no or short notice;

   viii. issues regarding the size of family trees that may need to be constructed to ultimately identify an individual, and the amount of personal information that may need to be collected to construct such family trees;

   ix. the possibility of 'scope creep' in the use of F/IGG to investigate less serious crimes which are currently not permitted according to the regulation of the DNA database vendors and may not meet with public expectations; and

x. issues regarding reference testing.

d. Consulted with the NSW Privacy Commissioner.

e. Consulted with the s 47F(1) at the s 47G(1)(b) s 47G(1)(b) noting that some of the key issued discussed included:

i. consent and implications for use of third-party vendors; it is important not be reliant upon the terms and conditions of the external vendors, and instead have robust, transparent and explicit policies outlining the permitted circumstances of use;

ii. powers to seek or compel reference testing; clear and defined standard operating procedures are required for reference testing, and consideration given to only permitted 'one to one' comparisons rather than uploading reference tests to the commercial databases; and

iii. the importance of procedures around the management, storage and collection of data to avoid misuse; incorporating clear structural boundaries in data storage to prevent leakage.

The issues raised during those consultation sessions have been taken into account by the AFP in designing the Project, and during the course of the PIA.

Appendix C – Glossary

Capitalised terms in this PIA have the meaning given below, unless the context requires otherwise:

AFP means the Australian Federal Police.

APP means Australian Privacy Principle.

APP Code means the *Privacy (Australian Government Agencies – Governance) APP Code 2017*.

APP Guidelines means the *Australian Privacy Principles guidelines*, issued by the OAIC.

Data Matching Guidelines means the *Guidelines on data matching in Australian Government administration*, issued by the OAIC.

DNA means deoxyribonucleic acid.

DNA Data means the DNA data generated via WGA or WGS by a private third party laboratory.

Familial Link Data means personal information about individuals that is generated following the uploading of DNA Data to third party DNA databases.

F/IGG means Forensic Investigative Genetic Genealogy, being a forensic technique that uses DNA analysis in combination with information available via public genetic databases, to support investigation processes used to identify human remains and perpetrators of crime.

Genetic Genealogy Database means GEDmatch PRO, FamilyTreeDNA and DNASolves.

OAIC means the Office of the Australian Information Commissioner.

Open Source Data means other data available to the AFP, against which to match Familial Link Data.

PIA means privacy impact assessment.

PIA Guide means the *Guide to undertaking privacy impact assessments*, issued by the OAIC.

Project means the project being undertaken by the AFP, in collaboration with NSW Police, Victoria Police and The Victorian Institute of Forensic Medicine, to assess the viability of F/IGG for operational implementation at a federal level by the AFP.

Privacy Act means the *Privacy Act 1988* (Cth).

Privacy Policy means a policy containing all matters required by APP 1.4.

Reference Testing Data means DNA data collected from an individual that is identified as a potential familiar link to unidentified human remains, or is identified as a potential perpetrator.

STR means short tandem repeat, being a DNA analysis technique.

WGA means whole genome arrays, being a DNA analysis technique.

WGS means whole genome sequencing, being a DNA analysis technique.

Appendix D – Material Reviewed

Australian Federal Police Privacy Impact Assessment Template, undated.

New South Wales Police Force Privacy Impact Assessment, dated 8 December 2022.

Privacy Threshold Assessment – Pilot use of Forensic/Investigative Genetic Genealogy for ACT cold case investigation, dated November 2022