NCFS
National Centre for Forensic Studies
UC | CIT | AFP

Model Privacy Impact Assessment for Forensic Phenotyping

ISBN 978-0-9872324-2-7

Ownership of intellectual property rights in this publication

Creative Commons Licence

Inquiries

Inquiries about this document should be directed to:

NCFS Director
National Centre for Forensic Studies
University of Canberra, ACT 2601
Australia
Contact Page

Date of publication

23 September 2017

Table of Contents

Creative Commons

Disclaimer of Liability

The authors and the National Centre for Forensic Studies, Canberra draw the reader's attention to section 5 of the Creative Commons Attribution-NonCommercial License:

a. Unless otherwise separately undertaken by the Licensor, to the extent possible, the Licensor offers the Licensed Material **as-is** and **as-available**, and makes no representations or warranties of any kind concerning the Licensed Material, whether express, implied, statutory, or other. This includes, without limitation, warranties of title, merchantability, fitness for a particular purpose, non-infringement, absence of latent or other defects, accuracy, or the presence or absence of errors, whether or not known or discoverable. Where disclaimers of warranties are not allowed in full or in part, this disclaimer may not apply to You.

b. To the extent possible, in no event will the Licensor be liable to You on any legal theory (including, without limitation, negligence) or otherwise for any direct, special, indirect, incidental, consequential, punitive, exemplary, or other losses, costs, expenses, or damages arising out of this Public License or use of the Licensed Material, even if the Licensor has been advised of the possibility of such losses, costs, expenses, or damages. Where a limitation of liability is not allowed in full or in part, this limitation may not apply to You.

c. The disclaimer of warranties and limitation of liability provided above shall be interpreted in a manner that, to the extent possible, most closely approximates an absolute disclaimer and waiver of all liability.

This document does not constitute legal advice.

About the National Centre for Forensic Studies

In 2003, Canberra Institute of Technology (CIT), the University of Canberra (UC), and the Australian Federal Police (AFP) signed a Memorandum of Understanding (MoU) that recognised the benefits that could be gained from close collaboration between the three organisations with respect to forensic science training, education and research.

The MoU prompted discussions regarding the establishment of a National Centre for Forensic Studies (NCFS). The Centre would be ACT-based but would operate at both a local and national level.

On 22 August 2007, a Memorandum of Agreement was signed by the three organisations to formally establish the NCFS.

NCFS Purpose

To develop and deliver enhanced education, training and research opportunities for the benefit of the partner agencies and the wider forensic science community.

NCFS Objectives

The key objectives of the NCFS are to:

- increase collaboration and co-investment on forensic research
- promote forensic expertise, innovation and service delivery nationally and internationally
- encourage closer collaboration on strategic planning and public policy development, workforce planning and training, and
- actively explore opportunities for cooperation and co-investment in physical, information, and communication technology infrastructure development.

Through continuing to invest in our strategic capabilities, the NCFS will position itself to provide leadership and contribute to the development of the forensic sciences to support the justice system.

The NCFS will, at all times, act in an ethical manner to meet the standards expected by our stakeholders and the wider community.

NCFS Vision

To be recognised, nationally and internationally, as a valued contributor to the forensic sciences through:

- integrity underpinned by adherence to ethical and professional best practice
- excellence in training by providing a one-stop shop to meet the needs of students and clients
- innovation in research, development and implementation of technologies relevant to the practice of forensic science
- leadership by contributing to public debate and policy affecting the forensic sciences, and
- development of current practitioners and the future workforce through education and training

Areas of Expertise

CIT, UC and the AFP each bring to the NCFS existing strengths and capabilities and are identifying and developing synergies for the delivery of a new range of capabilities and services. In addition to our core academic courses, the expertise and experience of the partners can be utilised to meet the needs of industry clients.

About the Authors

Nathan Scudder is a lawyer, and a postgraduate student at the University of Canberra, studying the legal, ethical and privacy implications of Massively Parallel Sequencing and Forensic Genomics. He is a member of the International Association of Privacy Professionals.

Dr James Robertson is a Professorial Fellow at the University of Canberra and the Director of the National Centre for Forensic Studies.

Dr Dennis McNevin is an Associate Professor of Forensic Studies at the University of Canberra, leading research in forensic genetics. This includes the extraction of DNA from difficult substrates, discrimination between different species based on their DNA, the prediction of phenotype from genotype and differentiation of human populations according to their biogeographical ancestry.

Dr Simon J. Walsh is National Manager Specialist Operations for the Australian Federal Police, having joined the agency in 2006. Prior to this, Dr Walsh held a variety of professional and academic positions in forensic science having begun his forensic career in 1994.

Dr Sally Kelty joined the University of Canberra in 2015 as part of the teaching and research faculty in Psychology. She has previously held a post-doctoral fellowship in Criminology/Social Sciences at the University of Tasmania and research and practice positions at the Department of Justice in Western Australia, the University of Western Australia and The Women's and Infant's Health Research Institute. Dr Kelty's teaching and research interests include forensic and criminal psychology, psychological methods in forensic studies and positive psychology.

Acknowledgements

Research for this Model Privacy Impact Assessment was supported by an Australian Government Research Training Program Scholarship and by the Endeavour Fellowships and Awards, a Department of Education and Training initiative.

The authors would also like to acknowledge the assistance provided by a range of individuals, including members of the Australian Federal Police Specialist Operations and Chief Counsel portfolios, in reviewing and commenting on this Model Privacy Impact Assessment.

Summary of Recommendations

No	Recommendation
1	Laboratories considering using this Model Privacy Impact Assessment (PIA) should: • Consider whether the approach taken by the authors suits the legislative requirements in the laboratory's own jurisdiction. • Adapt and amend the Model PIA to suit specific local requirements, technology differences and the applicable legal framework. • Circulate and discuss the PIA with relevant local and regional stakeholders. • Consider publishing the PIA on their website, or otherwise making it accessible to stakeholders and interested members of the public.
2	Any major change in the technology base for Massively Parallel Sequencing (MPS) which, for example, could lead to an operational capability to predict donor behaviour or diagnose tendencies, should trigger a new PIA.
3	Entities considering future technology change beyond the scope of this PIA, such as targeting genetic markers for behaviour or whole genome sequencing for forensic analysis, should consider whether another PIA is required.
4	Entities using MPS analysis should ensure that genetic information and, in particular, raw genetic data is appropriately secured to prevent unauthorised access, use or disclosure.
5	Entities using MPS analysis should keep court reporting processes and intelligence processes distinct, to maximise the opportunities to negotiate during discovery or subpoena processes and keep third-party genetic information off the public record wherever possible. Entities should also consider potential third-party access rights under freedom of information processes, where they are applicable.
6	When operationalising an MPS platform, entities should give consideration to appropriate awareness training for police or investigators. Results or reports from MPS platforms should, where practicable, allow for discussions and guidance to be given by the scientists to investigators tasked with making operational decisions based on the content. Additional explanatory information should also be included in reports, where possible, to aide in interpretation.
7	Any outsourcing or fee-for-service arrangement involving MPS technology should give consideration to privacy risks and, in particular, which obligations fall to which parties. Auditing or certification requirement could also be used to mitigate risk, where appropriate.

No	Recommendation
8	Any outsourcing, fee-for-service or other collaboration involving MPS should give careful consideration to risks of secondary use, such as the diversion of genetic data into research and development initiatives without informed consent. Similar considerations may apply where an operational laboratory runs an in-house research and development program.
9	Where an entity proposes to use MPS technology for reference samples, consideration should be given to deriving genetic information only from DNA markers useful for comparison purposes. Where this is not feasible, externally visible characteristics (EVC), bio-geographical ancestry (BGA) or any other medically sensitive information should be segmented with access restricted at the earliest opportunity during the analysis process.
10	Entities should consider relevant privacy safeguards when analysing samples of mixed origin using an MPS platform, where there is a known contributor such as a victim of crime. Similar policies of segmenting and restricting access to EVC, BGA or other medically sensitive information in raw genetic data should, whenever it is feasible, apply at the earliest opportunity during the analysis process.
11	Entities moving to an MPS platform should review their policies and procedures concerning obtaining consent from individuals, particularly volunteers, and whether any changes are needed to inform those consenting of any relevant new capabilities of an MPS platform.
12	An entity should consider whether to include, in any relevant consent form, information about rights of access to personal information. The entity should also consider advising donors that the entity will not proactively release any information as to health status, even if this health information is readily apparent from the genetic information.
13	An entity should ensure that, before using MPS operationally, the agency's privacy policy or other relevant governance provides necessary guidance about the use to which the agency may put genetic information obtained from discarded DNA. Importantly, this policy should specify that the entity will not proactively release genetic information or information as to health status, even if the donor of the sample later becomes known and even if this health information is readily apparent from the genetic information. Consideration should be given to how this aligns with any statutory requirement to release copies of results to the donor.
14	Entities should ensure that their implementation of MPS considers the possibility of inadvertent release of information such as biological parentage or genetic ancestry information, and mitigate this risk if possible. Entities should also balance the 'right not to know' with investigative priorities if considering the use of health information for identification purposes.

No	Recommendation
15	Entities should ensure that, before using MPS operationally, the agency's privacy policy is reviewed to ensure that there are no express assurances of anonymity or pseudonymity in relation to forensic identification sciences.
16	Entities adopting MPS in a staged manner, and later broadening application to more crime types or for the more efficient analysis of reference samples, should consider whether a new PIA is necessary. See also Recommendation 9.
17	Entities should ensure that processes for the handling of electronic and hardcopy records containing genetic information meet all relevant security standards and requirements, as well as any data retention or archiving requirements.
18	Entities should consider gathering feedback on any MPS analysis provided to investigators, and to consider strategies to enhance reporting and privacy compliance.
19	Entities should ensure that their privacy processes include steps to be taken in the event of a suspected genetic 'data spill' (deliberate or inadvertent), including taking all reasonable steps to contain any breach.
20	Entities should consider their approach to deleting or tightly restricting genetic data, in cases where it is possible to make an assessment that it does not (or no longer) has any probative value.

Background

This Model Privacy Impact Assessment (PIA) considers the introduction of forensic phenotyping and a move towards forensic genomics through a privacy lens. The Model PIA considers the privacy challenges and benefits, and puts forward some mitigation strategies to reduce identified risks.

Purpose of the model PIA

The Model PIA is a starting point for laboratories in the process of implementing new DNA capabilities based on massively parallel sequencing (MPS) or considering the use of forensic genomics more broadly. While intended to have broad application, the Model PIA must be adapted to individual laboratory requirements.

The PIA process is applied in many countries, and the approach to developing a PIA would generally be a good basis to consider privacy implications, even in jurisdictions where PIAs are uncommon. However, each jurisdiction has its own requirements in terms of privacy and legal risk, and a different approach may be required.

Consultation is a key component of the development of a PIA. While the Model PIA is the result of considerable stakeholder input, a proposal to implement new technology having a bearing on privacy should trigger consultation with institutional, local and regional stakeholders. Laboratories considering implementing enhanced DNA capabilities based on forensic genomics should consider which stakeholders should be consulted on the appropriateness of privacy and legal safeguards. This could include:

- Local and regional law enforcement agencies;
- Institution and government policy areas;
- The Judiciary;
- Prosecution services or the office of the District Attorney;
- Victim advocacy groups;
- Inmate support groups; and
- Privacy advocacy groups.

The development of a PIA should be a transparent process. Laboratories should consider publishing their PIAs on their institution's website or otherwise making the final PIA document accessible to stakeholders and the public.

Recommendation 1

Laboratories considering using this Model PIA should:

- Consider whether the approach taken by the authors suits the legislative requirements in the laboratory’s own jurisdiction.
- Adapt and amend the Model PIA to suit specific local requirements, technology differences and the applicable legal framework.
- Circulate and discuss the PIA with relevant local and regional stakeholders.
- Consider publishing the PIA on their website, or otherwise making it accessible to stakeholders and interested members of the public.

Scope

Legislative framework

The Model PIA is a generic document, but has been developed with some consideration of its applicability under the following frameworks:

- Australia (*Privacy Act* 1988 (Cth), incorporating the Australian Privacy Principles);
- the United Kingdom (*Data Protection Act* 1988, incorporating the UK Data Protection Principles);
- Europe, through the European Union Data Protection Directive 95/46/EC;
- the United States (the *Privacy Act of 1974* 5 U.S.C. § 552a, noting that it applies only to federal government department, corporations or establishments); and
- Japan (the *Act on the Protection of Personal Information held by Administrative Organs* 1988).

Existing state

The Model PIA considers the changes in the collection, use and disclosure of genetic information arising from the adoption of MPS or of a laboratory otherwise moving to make use of ‘coding’ regions of DNA. While phenotype prediction can apply to the interpretation of any human characteristic encoded in DNA, including health information of the donor, the term ‘forensic phenotyping’ is used in this Model PIA to distinguish the prediction of characteristics useful to forming an hypothesis as to an individual’s identity. These forensic phenotypes are predominantly externally visible physical features.

Forensic DNA analysis, using a select number of DNA loci for comparative purposes, was first used in 1987 in the United Kingdom. It was first used in the United States in 1989 and Australia in 1990.[1]

The Model PIA does not consider the privacy implications of this existing use of identity markers. Nor does it consider other developments in DNA analysis over this period, including field portable DNA capabilities and the use of databases to store and compare DNA profiles.

This current use of DNA, while having evolved considerably in the last thirty years, is considered a baseline for the purposes of this privacy analysis. As such, this Model PIA considers what would change, from a privacy perspective, if a forensic laboratory replaced or supplemented its use of identity markers for DNA analysis with MPS or forensic genomic capabilities.

This Model PIA does not consider the use of phenotyping for behavioural prediction. While there may be forensically relevant information that can be drawn from making predictions as to a diagnosis concerning an individual's behaviour or tendencies, current MPS capabilities are not presently set up to undertake this analysis. Given such predictive capabilities, if developed, are many years from operational use, this Model PIA will consider current and short-term technology developments.

Recommendation 2

Any major change in the technology base for MPS which, for example, could lead to an operational capability to predict donor behaviour or diagnose tendencies, should trigger a new PIA.

Technical Description

Current State

DNA analysis for law enforcement and forensic purposes has been in widespread use since the late-1990s.[2] This early adoption of DNA came with assertions that the points of analysis within the human genome constituted so-called 'junk DNA'.[3] This assertion has since been challenged, and certain variants detected with existing kits and markers can identify sensitive medical information and inherited genetic traits.

Despite these limitations, comparative DNA analysis has, over a period of about thirty years, shown itself to be a forensic tool with a high degree of genetic privacy compliance.

Privacy compliance is achieved through a range of internal laboratory practices and oversight mechanisms. In addition, once entered into a local or national DNA database, use of DNA profile information is often constrained by legislation or policy. By focusing on a numerical representation of short tandem repeats, most suited to upload and comparison in databases, forensic DNA analysis has largely side-stepped the issue of genetic privacy up until this point in time. There has been little incentive for individual laboratories or police agencies to move away from consistent, core DNA markers which can be readily compared to the same markers from unsolved crimes, suspects and convicted offenders.

Massively Parallel Sequencing and Forensic Genomics

Advances in genetic analysis have led to a generational shift in DNA processing capabilities. Laboratories are beginning to adopt new DNA systems based on Massively Parallel Sequencing (MPS). Drawing on medical research capabilities, MPS platforms allow for cost efficient analysis of an exponentially larger number of DNA markers. MPS has a range of uses, including genomic analysis of gene mutation associated with disease.[4, 5] In a forensic context, MPS can be beneficial in processing degraded DNA samples or providing raw data useful for the analysis of DNA mixtures. However, its most profound contribution will be in enabling investigators to predict genetically derived characteristics from genetic material of unknown origin.

It is logical to predict that forensic laboratories will continue to use existing DNA capabilities, or similar comparison-based genetic analysis using MPS, given that most crimes occur between people known to each other.[6] However, MPS is already proving itself a useful tool when traditional comparison based DNA fails to identify a suspect or convicted offender.

Information Flows

How is the genetic information collected?

The process of collecting DNA samples will not change through the introduction of MPS. Forensic laboratories are primarily adopting massively parallel sequencing (MPS) for use with unsolved crime scene samples.[7] DNA samples are generally collected by swabbing surfaces with which a suspect may have had contact, such as a door handle or a bladed weapon, or collecting apparent biological material of unknown origin. Sampling for DNA analysis may also occur in relation to victims of crime, such as through a medical examination following a sexual assault or as part of a post-mortem process.

Following an incident, a laboratory must determine which, if any, DNA samples will be analysed and in what sequence. The laboratory's aim is to conduct an efficient analysis so as to produce the most probative evidence or effective intelligence in relation to an incident. In doing so, a forensic scientist will consider a variety of factors, including the type of offence and any known pre-existing association between a suspect and the location of the crime.

Efficiency would be expected to be a strong driver of the platform used for analysis. Where a suspect is known to be associated with a location, conducting expensive trace DNA analysis would be a futile exercise. Likewise, a laboratory would likely favour fast and cost-effective processing of DNA samples to develop identification markers suitable for DNA database searches, if there is a reasonable prospect the unknown suspect will be identified through those database searches.

However, where it is not believed a suspect will be identified by database searches, or those searches are undertaken with nil results, the MPS platform provides a variety of additional capabilities to provide intelligence to investigators.

The MPS platform itself has wide application depending on the genetic targets employed by the MPS kit. It is therefore possible for an MPS instrument to be configured between runs to provide entirely different genetic information.[8]

The combination of all of these factors will determine whether a DNA sample generates:

- no information (that is, analysis of the sample reveals no usable genetic information);
- identification markers or a combination or mixture of markers, which may be suitable for database comparison;
- additional genetic information, with potential suitability for prediction of ancestry, surname, EVCs or prediction of medical status.

Surname and medical status prediction are evolving, the former being explored with both MPS platforms and other non-MPS technology. While these potential applications are considered in this PIA, the main privacy implications assessed relate to prediction of ancestry and EVCs. This

PIA does not consider moving beyond medical status prediction for identification purposes (for example, predicting whether an individual is likely to have been prescribed an unusual medication) to behavioural or psychological predictions for the purposes of profiling a suspect.

It should be noted that some potential uses cross these boundaries. Should reliable markers for gait or voice characteristics be identified, for example, there could be some dispute as to whether they are EVCs or behavioural predictions.

Recommendation 3

Entities considering future technology change beyond the scope of this PIA, such as targeting genetic markers for behaviour or whole genome sequencing for forensic analysis, should consider whether another PIA is required.

What genetic information is being held?

The FBI's CODIS database currently contains more than twenty DNA markers:[9]

- CSF1PO
- FGA
- THO1
- TPOX
- VWA
- D3S1358
- D5S818
- D7S820
- D8S1179
- D13S317
- D16S539
- D18S51
- D21S11
- D1S1656
- D2S441
- D2S1338
- D10S1248
- D12S391
- D19S433
- D22S1045
- AMXY

If a laboratory simply substituted an MPS-based platform for its existing DNA processing capabilities, using a suitable MPS kit containing only those markers, there would be little change to the baseline privacy position. The laboratory would simply be using a different method of DNA analysis to derive the same genetic information, for comparison with DNA obtained from suspects and victims through existing voluntary or coercive collection processes. While MPS-based platforms provide more sequence information, which may be phenotypically informative, such a one for one replacement technology would pose little additional privacy risk when compared to current DNA processing capabilities.

As previously discussed, derivation of genetic information at the twenty identity markers listed above is not entirely immune from privacy concerns. The familial nature of DNA, its identification of biological gender, and more recent research into whether some markers thought to be 'non-coding' could, in fact, inform some predictions, continue to present potential privacy issues. However, for the purposes of this PIA, these privacy considerations are also a feature of existing DNA capabilities which have remained unchanged for nearly 30 years.

One significant advantage of MPS-based platforms is the ability to process a significantly larger number of markers, many of which are specifically chosen as genetically informative markers.

For example, the *llumina® ForenSeq™* DNA Signature Prep Kit contains 94 autosomal human identity single nucleotide polymorphisms (SNPs), 27 autosomal short-tandem repeat (STR) markers, the sex-determining amelogenin marker, 24 Y chromosome STRs, 7 X chromosome STRs, 56 autosomal ancestry informative SNPs and 22 autosomal phenotype informative SNPs (for eye and hair colour). While still only the tiniest fraction of the human genome, these markers are sufficient to inform a range of phenotype and ancestry predictions.[10]

Analysis and access to genetic information

When compared to the existing state, MPS-based platforms reveal more genetic information to forensic scientists and, subject to existing and proposed controls, could potentially reveal more genetic information to investigators and the courts, either directly or derived from reporting of phenotypes. As noted, MPS can provide more sequence information than previous technologies. This, in part, is a product of the disparate uses of MPS and its more widespread use in fields of medical research.

Genetic information derived from MPS analysis could include information falling into three categories:

- *Raw genetic data:* Specific bases relating to the genome of an individual, known or unknown.

- *Processed genetic data* directly relevant to predictions of bio-geographical ancestry (BGA) or externally visible characteristics (EVC) of an individual, known or unknown.

- *Other processed genetic data*, should it become operationally feasible, predicting other individual attributes such as the hereditary medical status of an individual, known or unknown.

The *Privacy Act 1988* (Cth) classes genetic information as 'sensitive information'.[11] As such, in some circumstances it can be subject to additional requirements concerning its collection, use and disclosure. While the primary purpose of collection and use is to provide intelligence support to law enforcement investigations, primarily by assisting in identifying an individual through their genetic traits, the data itself poses other privacy risks once associated with a known individual:

- *Processed genetic data* concerning BGA or EVC could be used to identify or challenge an individual's cultural heritage or familial links.

- *Other processed genetic data* would be informative of other genetic conditions. While there is an argument that that information might assist law enforcement, it could also lead to other presumptions about an individual, such as their state of health.

- *Raw genetic data* poses two risks, depending on the specific markers analysed. It could be further analysed (either in isolation or with other genetic information known to be associated with an individual) to make predictions based on current research knowledge of the human genome. Alternatively, the data could be stored and analysed to make predictions based on future discoveries regarding the human genome.

The sensitive nature of genetic information therefore warrants an appropriate level of safeguarding. While used as the basis for intelligence product, the raw genetic data should be retained securely and be accessible only by authorised individuals. Entities using MPS could maintain these safeguards by examining workflows in the laboratory, identifying any points in the analysis or reporting process where a 'data spill' could occur or where unauthorised individuals could obtain access to genetic information.

Recommendation 4

Entities using MPS analysis should ensure that genetic information and, in particular, raw genetic data is appropriately secured to prevent unauthorised access, use or disclosure.

Further considerations may apply if MPS workflows could overlap with court reporting. While MPS may be employed for intelligence purposes, the platform can also be employed to analyse identification markers. Where this occurs, the possibility of raw genetic data falling into a court discovery or subpoena process should be considered. In many jurisdictions, court discovery processes are extensive and a key element of the justice system.

While existing DNA capabilities could require a laboratory to produce raw data (such as electropherograms) as part of a court process, those DNA capabilities were designed to select markers with minimal genetic privacy risks. MPS therefore carries greater risks to individuals, including the potential re-identification of other genetic datasets, if put on a public record.

Recommendation 5

Entities using MPS analysis should keep court reporting processes and intelligence processes distinct, to maximise the opportunities to negotiate during discovery or subpoena processes and keep third-party genetic information off the public record wherever possible. Entities should also consider potential third-party access rights under freedom of information processes, where they are applicable.

The privacy risks around processed genetic data for BGA or EVC primarily relate to how information is understood and used by those tasked with taking the intelligence product and actioning it. While phenotyping can be a valuable tool for investigators, privacy rights will only be maintained where its purpose and limitations are fully understood. Investigators may, for example, target a particular ethnic group based on BGA prediction. A 'dragnet' of individuals with particular physical characteristics could be attempted. Both of these approaches could undermine confidence in the technology and in jurisdictions such as the United States could result in legal challenge.

The release of information to investigators can represent a higher risk to privacy where:

- it reveals EVC or BGA prediction that is likely to be misinterpreted; or
- reveals information about an individual other than an EVC or BGA.

Recommendation 6

When operationalising an MPS platform, entities should give consideration to appropriate awareness training for police or investigators. Results or reports from MPS platforms should, where practicable, allow for discussions and guidance to be given by the scientists to investigators tasked with making operational decisions based on the content. Additional explanatory information should also be included in reports, where possible, to aide in interpretation.

Information sharing

Transfer of information from one entity to another can occur in two situations. The first is where an MPS capability is ‘outsourced’ or otherwise provided to law enforcement agencies on a fee-for-service basis. Such models could be all-inclusive, or could involve the use of an MPS platform followed by further data analysis by another entity (government or private sector) to generate additional intelligence information.

The second situation arises in relation to research and development, and involves collaboration efforts between different entities so as to enhance the predictive capabilities of an MPS platform.

The first situation can generally be managed by appropriate consideration of privacy and security requirements in any contractual arrangement. Where any outsourced or fee-for-service model is negotiated, both parties should assess how privacy and security requirements, and other privacy enhancements, can be implemented and which party bears the responsibility. Auditing or certification arrangements could also be considered, particularly where an entity believes that there is a high risk of reputational harm in the event of a ‘data spill’ or other privacy breach.

Recommendation 7

Any outsourcing or fee-for-service arrangement involving MPS technology should give consideration to privacy risks and, in particular, which obligations fall to which parties. Auditing or certification requirement could also be used to mitigate risk, where appropriate.

The second situation, involving research collaboration, requires even more careful analysis. It is unlikely that a victim or suspect in a criminal matter could be regarded as having consented to their genetic data being used for research, even where that data has been de-identified. Where data is to be shared between laboratories, extreme care would be needed to guard against inappropriate secondary use.

Recommendation 8

Any outsourcing, fee-for-service or other collaboration involving MPS should give careful consideration to risks of secondary use, such as the diversion of genetic data into research and development initiatives without informed consent. Similar considerations may apply where an operational laboratory runs an in-house research and development program.

Withdrawal of consent

The collection of personal information generally requires an individual's consent, and that consent can be withdrawn in certain circumstances.[12, 13] In the context of genetic information derived from DNA collected at crime scenes, and of unknown origin, issues of consent do not apply. If an entity proposes to use an MPS platform, particularly phenotype prediction, in relation to samples of known origin, issues of consent may become relevant.

The use of MPS for phenotype prediction for samples of known origin would appear nonsensical. There is no law enforcement benefit in predicting EVC or BGA for a person who is already known to police. However, the MPS platform itself could present cost benefits and economies of scale for forensic laboratories, compared to older DNA technologies. A laboratory may therefore elect to run a single model or type of MPS platform for both crime scene and reference samples.

Recommendation 9

Where an entity proposes to use MPS technology for reference samples, consideration should be given to deriving genetic information only from DNA markers useful for comparison purposes. Where this is not feasible, EVC, BGA or any other medically sensitive information should be segmented with access restricted at the earliest opportunity during the analysis process.

Consent would be relevant in relation to volunteers and contributors to known components of DNA mixtures, if their identity is or becomes reasonably apparent. While a victim of crime may, for example, agree to provide a reference sample to exclude their DNA profile from being uploaded from crime scene samples to a national DNA database, the question becomes more vexed when analysing a DNA sample of mixed origin using EVC or BGA capabilities. Some of the genetic data generated would be from the known contributor.

Guidelines issued by the Office of the Australian Information Commissioner require that entities subject to the *Privacy Act* 1988 (Cth) respond appropriately and, in most cases, make no further use of personal information if consent is withdrawn.[12] It is likely that a volunteer could expressly withdraw consent in relation to a reference sample, but not in relation to so-called discarded DNA. A component of that discarded DNA may have come from the volunteer, and may then be uploaded to a DNA database or subject to EVC or BGA prediction.

Recommendation 10

Entities should consider relevant privacy safeguards when analysing samples of mixed origin using an MPS platform, where there is a known contributor such as a victim of crime. Similar policies of segmenting and restricting access to EVC, BGA or other medically sensitive information in raw genetic data should, whenever it is feasible, apply at the earliest opportunity during the analysis process.

The processes around consent and withdrawal of consent are largely unchanged from previous DNA technology. However, as DNA analysis still has a high dependence on community cooperation, particularly of victims of crime, and a technology change could result in concern about misuse of genetic information, entities should carefully consider their approach.

Recommendation 11

Entities moving to an MPS platform should review their policies and procedures concerning obtaining consent from individuals, particularly volunteers, and whether any changes are needed to inform those consenting of any relevant new capabilities of an MPS platform.

Access to personal information

Individuals generally have a right to request access to their own personal information. See, for example, Australian Privacy Principle 12 in Sch 1, *Privacy Act 1988* (Cth); *Privacy Act of 1974* (US), § 552a(d); *Data Protection Act 1988* (UK), Part 2 and *Act on the Protection of Personal Information Held by Administrative Organs* (Japan), article 12. An individual may develop an interest in the genetic information held by an entity, either in raw form or in the form of analysis of EVC, BGA or other forensically relevant information. Entities will need to consider the relevant approach to releasing this information, assuming that no exemptions apply due to operational sensitivities at the time.

A right of access could arise in relation to reference samples, the known component of a DNA mixture obtained through a forensic procedure (generally performed on a victim of crime), or in relation to discarded DNA (including mixtures) collected from a crime scene and subsequently re-identified through an investigative process.

Reference samples and DNA obtained through forensic procedures

When taking reference samples for analysis with an MPS platform, entities have an opportunity to fully inform an individual and, except in the case of samples taken coercively, obtain relevant consent. The consent or information process can therefore detail the process applicable for subsequently requesting access to an individual's personal information.

Discarded DNA

Where samples are collected from discarded DNA and analysed using MPS (including prediction of EVC or BGA) normal consent arrangements would not apply. As such, an entity comes into possession of genetic information without any form of consent or an opportunity to provide information or disclaimers in relation to its use. This stands in contrast to other situations in which genetic information is usually obtained, such as medical testing or medical research.

Once re-identified, an entity may be asked by the donor to provide a copy of their personal information. More concerning, that individual may later seek legal redress against an individual, should the raw genetic information reveal genetic predisposition to disease.

Recommendation 12

An entity should consider whether to include, in any relevant consent form, information about rights of access to personal information. The entity should also consider advising donors that the entity will not proactively release any information as to health status, even if this health information is readily apparent from the genetic information.

Recommendation 13

An entity should ensure that, before using MPS operationally, the agency's privacy policy or other relevant governance provides necessary guidance about the use to which the agency may put genetic information obtained from discarded DNA. Importantly, this policy should specify that the entity will not proactively release genetic information or information as to health status, even if the donor of the sample later becomes known and even if this health information is readily apparent from the genetic information. Consideration should be given to how this aligns with any statutory requirement to release copies of results to the donor.

The right not to know

Current DNA reporting capabilities can lead to conclusions about biological parentage. The possibility of inadvertent release of information about whether a parent is biologically related has been an issue that forensic science has had to manage over many years. This issue became particularly relevant with the widespread use of DNA testing for missing persons or disaster victim identification.

MPS capabilities extend this risk into areas such as genetic ancestry information and potentially medically relevant information about individuals, known and unknown. There is at least some possibility that a suspect, identified through the use of EVC and BGA information from MPS, could develop a suspicion about their biological parentage if the police report differed from their own beliefs as to their genetic makeup.

Likewise, exploiting health status information for investigative purposes must be balanced carefully with the 'right not to know'. The Australian National Health and Medical Research Council notes that '*[i]t cannot be assumed that everyone will wish to know that they might have inherited a disorder present in their family'*.[14]

Recommendation 14

Entities should ensure that their implementation of MPS considers the possibility of inadvertent release of information such as biological parentage or genetic ancestry information, and mitigate this risk if possible. Entities should also balance the 'right not to know' with investigative priorities if considering the use of health information for identification purposes.

Anonymity/Pseudonymity

As with existing DNA technology, it is difficult if not impossible to assure anonymity or pseudonymity in a forensic DNA process. Indeed, the primary goal of forensic DNA analysis is to assist in identifying the likely donor of genetic material obtained in connection with a particular scene of crime.

Recommendation 15

Entities should ensure that, before using MPS operationally, the agency's privacy policy is reviewed to ensure that there are no express assurances of anonymity or pseudonymity in relation to forensic identification sciences.

Privacy Risks and Benefits

Community attitudes to genetic privacy

Genomic analysis and predictive health capabilities, whether used in a forensic, research or diagnostic setting, are highly dependent on the sharing of personal information by other individuals.[15] Indeed, very little could be gleaned from the human genome without a comparative analysis. The adoption of MPS capabilities for forensic purposes should adhere to community expectations on the use of genetic information. Given its reliance predominantly on discarded DNA from crime scenes, society must accept that their skin cells or other genetic material could be swept up and analysed without their knowledge or consent. The privacy checks and balances, therefore, are important to maintaining public confidence even though the public's attitude to genetic analysis is constantly changing.

New MPS capabilities

This PIA assumes that new MPS predictive capabilities will likely emerge in the future, becoming available as part of new or existing MPS kits. Laboratories themselves may not drive these changes, with instrument manufacturers potentially expanding kits to include analysis of different genetic markers.

Entities need to consider what processes should apply where new testing capabilities are made available, and how to ensure that any privacy intrusion is balanced against the perceived investigative benefit. There may be a temptation to provide as much information about an unknown crime scene sample to investigators as possible. However, this could result in undermining public confidence in the capability and reduced public cooperation with police investigations, particularly in the volunteers providing reference DNA samples.[16] Entities should consider *Recommendation 2*, above, concerning undertaking a new PIA if the capabilities of MPS significantly evolve.

Wider use of an MPS platform

Changes to the privacy impact are not necessarily confined to new MPS capabilities. A shift in the application of an MPS platform, from cold cases to all crime scenes, or from crime scene to reference samples, could also result in unforeseen consequences in terms of individual privacy, and may necessitate a new PIA process.

Recommendation 16

Entities adopting MPS in a staged manner, and later broadening application to more crime types or for the more efficient analysis of reference samples, should consider whether a new PIA is necessary. See also *Recommendation 9.*

Effect on DNA 'Dragnets'

DNA 'dragnets' or widespread sampling of a population to help solve a particular crime, has occurred in a number of countries. Sampling is almost always restricted to a small geographic area, based on the scene of the crime, and further restricted by gender or ethnic group (based on eyewitness evidence or, in the case of gender, potentially results of DNA analysis of the amelogenin genetic marker).

The use of MPS for EVC or BGA prediction in this instance may serve to more accurately refine the target population of a DNA dragnet, where it is appropriate. For example, where presently police may propose a dragnet of all male residents of a particular town, BGA or EVC could limit this intrusion based on prediction of appearance or ancestry. This, of course, must be considered carefully to avoid targeting of particular ethnic groups and, in the United States, consideration of the Fourth Amendment further restrains appropriate use of this technique.[16]

Compliance with Australian Privacy Principles

Australian Privacy Principle	How compliance requirements can be met
1 — open and transparent management of personal information	Compliance is achieved by conducting a PIA, documenting policies and procedures concerning use of MPS, and revising and reviewing documents through normal business practice.
2 — anonymity and pseudonymity	It is impractical for an entity assisting in identification in a forensic context to allow for anonymity or pseudonymity in most instances.
3 — collection of solicited personal information	Compliance (in relation to personal information and the further restricted sensitive information) is achieved by ensuring that collection is directly related to an entity's functions or activities and, further, that the entity is a relevant enforcement body.
4 — dealing with unsolicited personal information	This requirement is not generally applicable to MPS.
5 — notification of the collection of personal information	The notification of collection of genetic information to the original donor is generally not reasonable in the circumstances.
6 — use or disclosure of personal information	The release of any information derived from MPS analysis is made compliant by way of Australian Privacy Principle 6.2(b), concerning use or disclosure under an Australian law, or 6.2(e), concerning enforcement-related activities.
7 — direct marketing	Not applicable.
8 — cross-border disclosure of personal information	Cross-border disclosure could arise in circumstances where an entity outsources its MPS analysis or where it is necessary for an enforcement related purpose.

Australian Privacy Principle	How compliance requirements can be met
9 — adoption, use or disclosure of government related identifiers	Not applicable.
10 — quality of personal information	Given the predictive nature of EVC and BGA capabilities, it is reasonable for an entity not to maintain analytical information that is completely accurate.
11 — security of personal information	Compliance can be achieved by ensuring that information security requirements are adhered to.
12 — access to personal information	Entities can achieve compliance by ensuring that processes and procedures allow for reasonable access to MPS data and predictions (see *Recommendations 12, 13 and 14*).
13 — correction of personal information	Given the predictive nature of EVC and BGA capabilities, correction of personal information would not be expected to arise.

Compliance with United Kingdom Data Protection Principles

United Kingdom Data Protection Principle	How compliance requirements can be met
1 — personal data processed fairly and lawfully	Compliance is obtained as the data is required to be processed for the administration of justice.
2 — obtained for one or more specified and lawful purposes	Disproportionate effort would be required to notify unknown individuals of the collection of their personal data.
3 — adequate, relevant and not excessive	Compliance can be met by implementing processes and procedures to limit the data produced using MPS, or to de-identify or destroy any unnecessary genetic data, where lawful and appropriate.
4 — accurate and, where necessary, kept up to date	Given the predictive nature of EVC and BGA capabilities, it is reasonable for an entity not to maintain analytical information that is completely accurate.
5 — not be kept for longer than is necessary	Certain genetic information and analysis from MPS may need to be retained in accordance with other legal requirements or for court purposes.
6 — processed in accordance with the rights of data subjects	Entities can achieve compliance by ensuring that processes and procedures allow for reasonable access to MPS data and predictions (see *Recommendations 12-14*), and ensuring that data is not shared or disclosed (see *Recommendations 4-8*).

United Kingdom Data Protection Principle	How compliance requirements can be met
7 — unauthorised or unlawful processing or accidental loss	Entities can achieve compliance by ensuring that processes and procedures allow for reasonable access to MPS data and predictions (see *Recommendations 12, 13 and 14*).
8 — international transfer outside of the European Union	Cross-border disclosure, outside of the European Union, could arise in circumstances where an entity outsources its MPS analysis or where it necessary for an enforcement related purpose.

Risk Mitigation Strategies

‘Masking’, encrypting or segmenting personal information

(See also Recommendations 5, 9 and 10)

A key element to ensuring community confidence in the forensic use of MPS is to ensure that personal information or data is handled appropriately. A crime scene examiner or forensic laboratory analyst cannot visually distinguish between the genetic material of a suspect, victim or bystander. Only by exploiting the sample to derive genetic information can conclusions be made about the possible origin of genetic material.

As the forensic process continues, the segmenting, deletion, masking or encryption of data no longer necessary to the forensic process can be a valuable tool to protect individual privacy.

This approach could include:

- tight controls about who can access the raw genetic data developed through an MPS process;
- early deletion of markers not related to DNA database identification, where legally permitted, if a laboratory chooses to use an MPS platform for reference samples and does not use a separate kit excluding those markers from analysis;
- restricting access to EVC, BGA or other non-DNA database markers for crime scene samples, until the identification markers have been compared to reference samples for the case and other available DNA databases.
- delineation between raw genetic data and processed analytical information (intelligence), when releasing that information to investigators or the general public.

Release of information to the courts

Courts will also need to consider the way in which genetic information from MPS will be introduced into proceedings. While genetic information may fall within the ambit of a subpoena or a discovery process, segmenting the data will make decisions of courts or tribunals far easier than if raw data and processed data relating to a range of individuals is intertwined in a case file. Courts can then make informed decisions about how, for example, the genetic information of a victim from a mixed source profile will be managed during a trial process. While the discovery and subpoena processes can be extensive, it is within the power of the courts to exert a level of control of how information is to be managed, including ordering non-disclosure.

Such court control can help mitigate against instances where full disclosure is relevant in the interests of justice, but where disclosure could be to the detriment of the privacy of other individuals, such as victims of crime.

Freedom of information Act and other rights of access

Similar considerations apply in relation to other means of obtaining information held by an entity. Segmenting genetic information will make managing such requests, including requests by an individual for their own personal information, far less complex. Adopting clear processes for information management provides a range of privacy and information access benefits throughout the forensic process.

Information security

Privacy laws generally put entities under an obligation to manage the security of personal information, and require action to be taken in relation to any unauthorised release of information (a ‘data spill’). Entities can reduce risk by implementing appropriate security protocols around both electronic and hardcopy records.

Recommendation 17

Entities should ensure that processes for the handling of electronic and hardcopy records containing genetic information meet all relevant security standards and requirements, as well as any data retention or archiving requirements.

Forensic Reporting

(See also Recommendation 6)

MPS analysis yields intelligence outcomes for investigators. The inappropriate targeting of individuals based on EVC or BGA, or other privacy intrusions, can best be managed by training and education of investigators, as well as ensuring that those consuming intelligence products have direct access to forensic scientists to explain the relevant report and the underlying statistical model.

An entity implementing an MPS platform should consider feedback processes from the end consumers of their analysis. This feedback can assist in refining their reporting format.

Recommendation 18

Entities should consider gathering feedback on any MPS analysis provided to investigators, and to consider strategies to enhance reporting and privacy compliance.

De-identification and re-identification

The potential for genetic data to be re-identified, by aggregation or comparison with other available datasets, adds to the privacy risk.[17, 18] An approach that 'masks', segments or encrypts genetic data during the forensic process will help to mitigate this (see *Recommendations 5, 9 and 10*). Likewise, ensuring compliance with security requirements concerning electronic and hardcopy records (*Recommendation 17*) helps to ensure that genetic information will not fall into the wrong hands.

Recommendation 19

Entities should ensure that their privacy processes include steps to be taken in the event of a suspected genetic 'data spill' (deliberate or inadvertent), including taking all reasonable steps to contain any breach.

Deletion

The timely deletion of genetic data requires a careful balancing of:

- individuals' rights and expectations concerning their personal privacy, particularly if they are found not to be associated with a criminal activity;
- the entity's quality assurance requirements and interest in maintaining raw genetic data in a form that can assist with detecting and remedying any quality concerns;
- discovery and disclosure obligations to the courts or other oversight bodies.

While it may be possible to omit certain genetic information (such as genetic marker details concerning a bystander or a victim of crime) from analysis and reporting, entities would need to carefully consider whether deletion of raw genetic data is lawful and feasible, particularly with respect to disclosure, data retention or archiving requirements. An approach of tightly restricting access to genetic data may be preferable.

While actual deletion of data may not be feasible, access to genetic data that is not probative or relevant to a case could be so tightly restricted as to approach *logical deletion* (for example, restricting access to the laboratory quality manager or IT administrator).

Recommendation 20

Entities should consider their approach to deleting or tightly restricting genetic data, in cases where it is possible to make an assessment that it does not (or no longer) has any probative value.

Conclusions

There are a number of practical steps that an entity can take in implementing MPS for forensic use, so as to ensure both adherence to any applicable privacy laws and overall minimisation of intrusion to personal privacy. MPS provides many opportunities for law enforcement. However, maintaining public confidence in the technology will be critical to its successful implementation and use.

Stepping through the various recommendations of this Model PIA, as they apply to an entity, will assist in determining how a privacy compliant framework can be put in place for MPS analysis of both crime scene and reference samples.

As with any technology, new capabilities will evolve over time. These capabilities may enhance or challenge assumptions as to personal privacy. It is also important to review privacy compliance periodically and, in particular, before any broadening of the technical capabilities or application of MPS within a forensic setting.

References

[1] M. Smith, DNA Evidence in the Australian Legal System, LexisNexis Butterworths, 2015.

[2] D. Gusella, No Cilia Left Behind: Analyzing the Privacy Rights in Routinely Shed DNA Found at Crime Scenes, BCL Rev., 54 (2013) 789.

[3] J.K. Wagner, Out with the “Junk DNA” Phrase, Journal of Forensic Sciences, 58 (2013) 292-294.

[4] C.G. Chute, M. Ullman-Cullere, G.M. Wood, S.M. Lin, M. He, J. Pathak, Some experiences and opportunities for big data in translational research, Genetics in Medicine, 15 (2013) 802-809.

[5] M. Gloudemans, N. Shamaprasad, Current Issues in Forensic DNA Applications. http://www.pged.org/wp-content/uploads/2015/04/Current-Issues-in-Forensic-DNA-Applications.pdf, 2015 (accessed 17.05.16).

[6] E. Murphy, Legal and ethical issues in forensic DNA phenotyping, New York University Public Law and Legal Theory Working Papers. Paper 415, (2013).

[7] K. Lester, DNA testing by University of Canberra forensics lab to make molecular sketches of crime suspects, 666 ABC News, (2016).

[8] C. Børsting, N. Morling, Next generation sequencing and its applications in forensic genetics, Forensic Science International: Genetics, 18 (2015) 78-89.

[9] Federal Bureau of Investigations, Frequently asked questions on CODIS and NDIS. https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (accessed 17.06.17).

[10] A.D. Ambers, J.D. Churchill, J.L. King, M. Stoljarova, H. Gill-King, M. Assidi, M. Abu-Elmagd, A. Buhmeida, B. Budowle, More comprehensive forensic genetic marker analyses for accurate human remains identification using massively parallel DNA sequencing, BMC genomics, 17 (2016) 21.

[11] Privacy Act 1988 (Cth), in.

[12] Office of the Australia Information Commissioner, Australian Privacy Principles guidelines, (2015).

[13] Act on the Protection of Personal Information Held by Administrative Organs (Japan), in, 2003.

[14] National Health and Medical Research Council, Ethical aspects of human genetic testing: an information paper, (2000).

[15] E. Vayena, U. Gasser, Between openness and privacy in genomics, PLoS Med, 13 (2016) e1001937.

[16] E. Murphy, Inside the Cell: The Dark Side of Forensic DNA, Nation Books, New York NY, 2015.

[17] B. Malin, L. Sweeney, Re-identification of DNA through an automated linkage process, in: Proceedings of the AMIA Symposium, American Medical Informatics Association, 2001, pp. 423-427.

[18] M.D. Edge, B.F.B. Algee-Hewitt, T.J. Pemberton, J.Z. Li, N.A. Rosenberg, Linkage disequilibrium matches forensic genetic records to disjoint genomic marker sets, Proceedings of the National Academy of Sciences, (2017).