DNA databases in Australia and New Zealand
May 2016

As genetic technologies advance, countries across the world are seeking to establish DNA databases. Such databases can be a crucial tool for the prevention and detection of criminal activity and, with the appropriate safeguards, can reinforce and support the enjoyment of human rights. Without proper safeguards, however, large government databases of incredibly sensitive personal information pose untold risks to the enjoyment of the rights to privacy and data protection.

There remains a paucity of authoritative statements from international human rights mechanisms regarding the demands of human rights law in the context of such databases. However, it is possible to derive some human rights standards from European Court of Human Rights jurisprudence, particularly the *S and Marper v United Kingdom* judgement. In addition, the Forensic Genetics Policy Initiative has been monitoring the implementation and use of DNA databases for many years and has drafted a set of best practices which we believe DNA databases laws and practices should comply with. In this briefing, we use the best practices as a guide to analyse the DNA databases maintained by Australia and New Zealand, and to assess the laws and practices for their compliance with human rights standards.

I. SUMMARY AND COMPARISON

= Laws conform with best practices
= Laws conform with best practices, with some exceptions
= Laws contravene best practices
= Insufficient information available

	PRACTICE	AUS	NZ
1.1.	**Collection of DNA**		
1.1.1	Collection of DNA with consent from volunteers		
	Fully informed consent required		
	Only for a specific investigation, no database entry		
	Written consent required		
1.1.2	Collection of DNA w/o consent from suspects and convicted persons		
	Prior authorisation		
	Authorisation based on evidence of "probable cause" or equivalent		
	Restricted to serious crimes only		

	Sample/profile of suspects who are acquitted or not charged must be removed		
1.2.	**Destruction of DNA and linked data**		
1.2.1.	Destruction of biological samples		
	All samples destroyed after DNA profiles derived (after temporary retention)		
1.2.2.	Destruction of innocent people's DNA profiles		
	Automatic process for removal of database records of innocent persons		
1.2.3.	Retention periods for DNA profiles of persons convicted of minor crimes		
	Retention limits in place for persons whose DNA is taken on conviction/in custody for minor crimes		
1.2.4.	Appeal process against retention		
	Independent and transparent process to request removal of records		
1.2.5	Deletion of linked data		
	Automatic deletion of linked data on other databases when DNA profiles destroyed		
1.2.6.	Exceptions for national security		
	Any national security exceptions should be clearly defined, debated and overseen		
1.2.7	Retention of crime scene evidence		
	Retain crime scene DNA evidence in case a re-investigation is needed		
2.1.	**Collection of biological samples**		
	Intimate samples to be taken with consent by medical professionals		
	Non-intimate samples to be taken by trained staff		
	Provision of particular procedures for vulnerable persons		
2.2.	**Provision of information**		
	Requirement to provide information to individuals		
3.1.	**Crime scenes and chain of custody**		
	Quality assurance procedures in place		
	Only trained crime scene examiners to collect DNA evidence		
3.2.	**Analysis of DNA for forensic purposes**		
	DNA analysis should only take place in forensic laboratories		
	Quality assurance procedures in place		
3.3.	**Provision, status and oversight of forensic laboratories**		
	Forensic laboratories are independent of the police		
	Independent oversight mechanism in place		
3.4.	**DNA profiling**		
	Profiling standards must be sufficient to minimise false matches		
3.5.	**Elimination databases**		
	A separate elimination database is kept for police, lab and medical workers		
	Provisions for deletion of staff DNA profiles when retention no longer necessary		
	Searches of elimination database confined to necessary to identify contamination		
4.1.	**Storage of DNA profiles**		
	DNA profiles are extracted based on "non-coding DNA"		
4.2.	**Separation of criminal and non-criminal databases**		

	Definition of missing person included in legislation		
	Missing persons' DNA databases to be separate from criminal database		
	Fulling informed consent required from relatives of missing persons		
	Provisions for destruction of biological samples when no longer needed		
	Provisions for deletion of profiles on request or at end of investigation		
4.3.	**Governance**		
	Independent and transparency system of governance in place		
	Publication of regular reports and information		
4.4.	**Access restrictions and security of data**		
	Access to DNA databases and biological samples is restricted		
	Provisions for secure transfers of data		
	Personal identification information should not be sent with samples to laboratories		
	Data protection law in place		
4.5.	**Restrictions on uses of stored data**		
	Use of DNA databases restricted to solving crimes and identifying dead bodies/parts		
	Separate restrictions on missing persons database		
	Any use of database for research is restricted to anonymised verification of database performance		
	Independent ethics board must oversee applications for research		
	No research for other purposes (health research, behavioural research etc)		
4.6.	**Restrictions on the use of familial searching**		
	Familial searching is restricted to serious, unsolved crimes		
5.1.	**Use of DNA evidence in court**		
	Prosecutions using DNA evidence must be supported by corroborating evidence		
	DNA evidence adduced at trial should be accompanied by warnings as to the possibility of contamination		
	DNA evidence is accessible by the defence		
5.2.	**Access to DNA evidence in the event of an appeal**		
	Individuals have the right to request reanalysis of crime scene forensic evidence in the event of appeal against conviction		
	Crime scene evidence used to convict individuals should be retained		
6.1.	**Sharing of DNA profile matches overseas**		
	Requirement that foreign country meets equivalent safeguards		
7.1.	**Penalties**		
	Penalties exist for contravention of DNA database laws		

II. AUSTRALIA

a. Overview

Each of Australia's seven states and two territories maintains a DNA database, regulated by State or Territorial law, each applicable to a distinct State or Territorial police force. The cross-border collaboration of and exchange of information between State police forces is coordinated by a federal agency, CrimTrac, pursuant to an Inter-Governmental Agreement signed by Federal, State and Territory law enforcement ministers in July 2000. In order to

enable police to check and compare profiles across States, CrimTrac maintains the National Criminal Investigation DNA Database (NCIDD), which has only been fully functional across Australian States and Territories since 2009. The NCIDD contains more than 917,000 profiles, facilitating in 2014-2015 more than 31,000 links between crime scenes and individuals.[1] Once added to the NCIDD database, DNA profiles are never removed. However, NCIDD profiles are all de-identified, meaning the NCIDD does not contain personal information and cannot identity any individual other than the sex determinant. The NCIDD does not contain any fields that are normally referred to as identity details such as names, addresses, dates of birth; or personal markings (tattoos, scars, eye colour, height, or weight).

In 2015, the NCIDD was upgraded to include additional capabilities. This database will be among the most advanced in the world, incorporating familial searching and kinship matching capabilities.[2]

Each State and Territory in Australia has separate legislation regulating the taking, analysis, retention, use and destruction of DNA samples. The Commonwealth legislation is the closest in stature to a Model Bill produced by the Standing Committee of Attorneys-General in 2000, and is seen as the exemplar in Australia, although provisions of some of the State and Territorial legislation arguably provide stronger protections.[3]

The threshold requirements and categories of persons who are liable to provide a DNA sample differ widely across the jurisdictions, as do the rights and entitlements regarding consent, withdrawal of consent, and retention and destruction of material. On the other hand, the procedures for carrying out the taking of DNA samples and other forensic material are relatively standardised across Australia, including regulation relating to the prohibition of questioning during sampling, the use of force, the persons qualified to take samples, and the recording of forensic procedures. Each of the jurisdictions also provides strong restrictions regarding the circumstances in which DNA profiles can be matched, and also elaborates numerous criminal offences regarded the unlawful retention of and access to samples and profiles, as well as the failure to destroy samples.

All jurisdictions make provisions for interim orders for the immediate carrying out of forensic procedure, where the probative value of evidence obtained because of the forensic procedure concerned is likely to be lost or destroyed if there is delay in carrying out the procedure. Interim orders can be made by phone or fax as well as in person.

There is a relatively harmonised approach across all jurisdictions with respect to the removal of identifying information relating to DNA profiles of volunteers, which must take place within 12 months after the DNA profile is placed on the DNA database (see, for example, s23YDAG *Crimes Act 2014* (Cth)). In some States, the identifying information of acquitted suspects must also be removed from the profile; in Queensland, for example, it is

1 CrimTrac Annual Report 2014-2015, p. 22, https://www.crimtrac.gov.au/sites/g/files/net526/f/CrimtracAnnualReport2015_8.pdf?v=1446084987

2 http://aic.gov.au/publications/current%20series/tandi/501-520/tandi506.html

3 *DNA Forensic Procedures: Further Independent Review of Part 1D of the Crimes Act 1914,* 30 June 2010. The Model Bill is found at Model Criminal Code Officers Committee, *Final Draft: Model Forensic Procedures Bill and the Proposed National DNA Database* (2000), Standing Committee of Attorneys-General, Canberra.

an offence to record identifying information on a DNA profile after the time at which samples should have been destroyed, including samples from acquitted persons (s530).

Every State makes reference to the maintenance of DNA databases, but neither the Commonwealth Act, nor many of the State acts, make reference to the relationship between State databases and the CrimTrac NCIDD. Information received through freedom of information enquiries of the Victorian police reveals that there is a strong move towards having only one database, the NCIDD. While the Victorian Police in the past have maintained a local database (GeneLink), when the Police changed its DNA kit to Promega Powerplex 21, with which Genelink does not have interoperability, the Victorian Police moved to using the NCIDD as its only database. In response to enquiries, Queensland, NSW and Western Australia confirm they also utilise the NCIDD as their primary database.

In November 2014, the Australian Minister for Justice, the Hon Michael Keenan, announced that Australia had entered into a pilot program with the United Kingdom, the United States and Canada enabling international sharing of DNA profiles.[4]

In Australia, legislation exists at both a federal (commonwealth) level as well as in each of the States and territories. For the purpose of this briefing, we look briefly below at the legislation applicable at the federal level. Part 1D of the Commonwealth C*rimes Act of 1914*[5] regulates the taking, use and destruction of fingerprints and DNA samples by the Australian Federal Police. Part 1D has been subject to a number of reviews, notably the Sherman Review in 2003, and the Further Independent Review in 2010.

Suspects

Non-intimate forensic procedures (the taking of a hair that is not a pubic hair and the taking of fingerprints) can be carried out on suspects without their consent, on the order of a senior constable, provided the suspect is in custody and there are reasonable grounds to believe the suspect has committed a relevant offence for which the procedure will produce evidence relevant to the suspect's role (s23WM-s23WO).

With respect to intimate forensic procedures (the taking of blood or a buccal swab) carried out on suspects, whether or not they are in custody, a magistrate can order the carrying out of a forensic procedure if he or she is satisfied on the balance of probabilities that the person on whom the procedure is to be carried out is a suspect and may have committed a relevant offence, and there are reasonable grounds to believe the forensic procedure will produce evidence useful in determining the suspect's liability for the offence (s23WT*)*. The magistrate must take into consideration the public interest, and have regard to the circumstances of the relevant offender's case (including age, physical and mental health, cultural background and religious beliefs). If the suspect is not in custody, the magistrate may issue a summons or a warrant, if justified (s23WW). If the suspect is a child, incapable person or Aboriginal person or Torres Strait Islander they must be represented by an interview friend and may also be represented by a legal practitioner (s23WX).

4 Marcus Smith and Monique Mann, "Recent developments in DNA evidence", T*rends and issues in crime and criminology justice no. 506*, 15 November 2015, available at http://aic.gov.au/publications/current%20series/tandi/501-520/tandi506.html

5 Available at http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/

DNA samples must not be taken while a suspect is being questioned (s23XIA). A person authorised to take the sample may use reasonable force to enable the sample to be taken or to prevent loss, destruction or contamination of the sample (s23XJ).

After a period of 12 months has elapsed since the taking of the forensic material, if proceedings have not been instituted against the suspect, or have been discontinued, the forensic material must be destroyed as soon as practicable unless a warrant for apprehension of the suspect has been issued (s23YD).

Convicted offenders

Authorised persons can take non-intimate forensic samples from serious offenders where they have informed consent or an order of a constable (s23XWC), and intimate forensic samples where they have the informed consent or an order of a magistrate (s23XWD). Informed consent can only be given after an offender is informed of a number of factors (s23XWJ) and given the opportunity to communicate with a legal practitioner of the offender's choice (s23XWG).

A serious offence means an offence under a law of the Commonwealth, or a State offence that has a federal aspect, punishable by a maximum penalty of imprisonment for life or 5 or more years (s23WA). Forensic samples taken from offenders are to be retained unless the conviction is quashed, in which case any forensic material must be destroyed (s23YDAA).

Volunteers

Authorised persons are authorised to carry out forensic procedures on volunteers provided they have their informed consent; if the person is a child or incapable person, their parent or guardian may give consent and the child or incapable person does not resist the carrying out of the procedure (s23XWQ). If a volunteer withdraws consent after the taking of the sample, a magistrate may order the forensic material be retained under certain circumstances (s23XWV).

Victims

There is no provision made for taking DNA from victims.

DNA database system

The *Crimes Act 1914* also makes provision for the maintenance of a DNA database system of DNA profiles derived from forensic material. The database will contain a "crime scene index", including DNA profiles derived from forensic material from victims and places where offences occurred; and indexes for missing persons, unknown deceased persons, serious offenders, suspects, volunteers (both limited and unlimited purposes) and a statistical index. Section 23YDAF stipulates the purpose for which DNA profiles within one index of the system can be matched with DNA profiles of other indexes.

There is no specific provision authorising the creation of DNA profiles. However, the Act makes it an offence to derive a DNA profile for inclusion on the system from forensic material required to be destroyed, and to derive a DNA profile from material that is *not "*excluded forensic material", which includes material found at a crime scene, taken from a suspect, offender or volunteer, taken from a deceased person or a missing person

(s23YDAD). Although the construction of the language is confusing, this seems to suggest that a DNA profile can be derived from forensic material collected in accordance with the legislation provided that material is not required to be destroyed.

DNA profiles on the volunteers (both unlimited and limited purposes) indexes must be removed from the system as soon as practicable after the end of the identifying period for the profile (12 months) (s23YDAG), and that profiles of offenders whose conviction has been quashed also be removed. Access to the DNA database is only permitted if the access is for the purpose of forensic comparison under a law of a State or Territory, and the comparison is for a permitted purposes (s23YUG).

b. Issues of concern

Retention of innocent persons' DNA

In South Australia, Western Australia and the Northern Territory innocent person's DNA samples can be retained indefinitely, whereas other states have provisions for the destruction of suspect's samples when they are not charged or convicted after a certain time period. The Australian Capital Territory puts the obligation on the suspect to apply to have their material destroyed after the completion of proceedings (s92). With respect to samples taken from convicted offenders, volunteers and in other circumstances, samples are able to be retained at the jurisdictional lab indefinitely.

Indefinite retention of DNA profiles

Generally speaking, there is no obligation to destroy DNA profiles derived from forensic material in any of the States or Territories after any period of time or in any circumstances. Most of the pieces of legislation in Australia adopt extremely complicated wording in provisions related to the creation and destruction of DNA profiles (as distinct from samples), obfuscating the reality of retention of DNA profiles. For example, in the Commonwealth and New South Wales legislation, there is no lawful authority to derive a DNA profile from a forensic sample, but the Acts create offences for those who provide material to enable the creation of DNA profiles from samples that should otherwise be destroyed (where, for example, a suspect has been acquitted).

National DNA Investigative Capability

CrimTrac, the federal authority managing the NCIDD, reports that it is rolling out a "National DNA Investigative Capability project" which "will deliver a strategic DNA investigative capability platform… enabl[ing] CrimTrac's law enforcement partners to utilize DNA technology within their state or territory legislation and policies. There is no more public information available about this project or explaining how it differs from the National Criminal Investigation DNA Database.

Elimination database

There does not seem to be provision under any of the legislative regimes for the establishment of elimination databases.

III. NEW ZEALAND

c. Overview

The Criminal Investigations (Bodily Samples) Amendment Act expanding New Zealand's database was passed in October 2009. Previously samples could be taken only from volunteers, people charged with crimes carrying sentences of seven years or more, or by order from a judge. The resulting law, the Criminal Investigations (Bodily Samples) Act 1995, allows the police to take samples from anyone they intend to charge with an imprisonable offence.

The 2008 Interpol survey reports that 20,170 crime scene DNA profiles and 85,300 individuals' profiles were held in New Zealand at the time of the survey.

Suspects

Under the Criminal Investigations (Bodily Samples) Act, a DNA sample can be taken from any person suspect of an offence specified in Part 3 of the Schedule to the Act, which includes offences related to weapons, indecent acts, assault, and cruelty to a child (s5(a)). The suspect must either give consent or be subject to a suspect compulsion order (s5(b)). A juvenile suspect between the ages of 14 and 17 can also give a DNA sample by consent or subject to a juvenile compulsion order.

An application for a compulsion order must be made before a District Court Judge (s13) and must set out why the requesting officer has good cause to suspect the individual of the offence and tor require a bodily sample. There is a prohibition against publication of the name of the individual subject to a compulsion order (s14).

Child suspects can consent to providing buccal samples only (Part 2A).

Persons charged with an offence

A bodily sample can be taken from a person charged with an imprisonable offence, or an offence listed in Part 3 of the Schedule (see above) if the person is in custody (s24J(1)(a)). A sample can also be taken from a person who a police officer intends to charge with an imprisonable offence or an offence listed in Part 3 of the Schedule.

Convicted persons

Police can serve a databank compulsion notice on any person convicted of an imprisonable offence or offence against Part 3 of the Schedule (s39).

Destruction of samples

All bodily samples and related identifying particulars are to be destroyed as soon as practicable after the expiry of the period of 24 months beginning on the date on which the sample is taken, if the person is not charged with the offence in relation to which the sample was taken, or a related offence, before the expiry of that period (s60(1)(d)). If a person is charged with such an offence before the expiry of that period, as soon as possible after the charge is withdrawn or the person is acquitted of the offence (s60(1)(e)). If the person is convicted, and the offence is not an imprisonable offence or in Part 3 of the Schedule, as soon as possible after the appeal period (s60(1)(f)). In all other circumstances,

the sample is to be retained only as long as it takes to derive a DNA profile from the sample, and should then be destroyed (s60(2A)).

DNA database

The police may maintain a DNA profile databank of DNA profiles derived from samples taken according to the Act (s25). The following information may be stored on the DNA databank:

- Any DNA profile derived from a sample taken from a person where the person is convicted of the offence in respect of which the sample is taken, or of a related offence, unless the conviction is subsequently quashed (s26(a)(i));
- Any DNA profile derived from a sample taken from a young person, where that person is convicted of an imprisonable offence or offence in Part 3 of the Schedule and a sentence is imposed or an order made by a Youth Court;
- Any DNA profile derived from a sample taken from a young person where a Youth Court makes an order discharging the charge and the offence is a relevant offence (s26).

With respect to DNA profiles pertaining to young persons, section 26A contains a schedule of retention periods requiring the profiles to be destroyed at particular times after conviction. In addition, certain young persons may apply for removal of DNA profiles from the database (s26B).

There is no provision for the retention of DNA profiles of suspects or non-convicted persons in the database.

In addition, police can establish a temporary databank in which DNA profiles derived from bodily samples can be stored until and prior to circumstances arising requiring the destruction of a DNA profile or its storage on the DNA profile databank (s24P).

Familial searching

The relevant Act provides that profiles in the DNA profile databank or temporary databank can only be accessed for the purpose of forensic comparison in the course of a criminal investigation by Police, as well as for the purpose of administering the databank and making information available under the Privacy Act 1993. The Act does not speak to the way in which searches of the databank can be done. However, it is known that New Zealand has been conducting familial searching since 2004. There have been a total of 36 cases involving familial searches and a total of 62 searches in those 36 cases (some cases have involved multiple searches). Two people have been convicted as a result of such a search. Of the 36 cases, 20 were historical.31 Each search has involved crimes of a serious nature, such as sexual assault, murder and arson.3Such statistics suggest this technique is currently only being utilised in New Zealand in exceptional circumstances.[6]

d. Issues of concern

Lack of legislative underpinning

[6] http://www.otago.ac.nz/law/research/journals/otago065282.pdf

The Criminal Investigations (Bodily Samples) Act regulates the taking of samples, the creation of DNA profiles and the maintenance of DNA databases. However, there are numerous areas of practice and policy with respect to DNA databases in New Zealand which do not seem to enjoy any regulatory or legislative underpinning. These include, for example, the provision, status and oversight of forensic laboratories, and the forensic processes for analysing DNA samples. There is little provision in the Act for processes regarding the taking of evidence at crime scenes and the preservation of chain of custody. There is no legislation relating to the need for secure transfers of data, or requiring that personal information not be sent with samples to laboratories.

Elimination database

The Act does not make any provision for an elimination database for the DNA of police officers, medical workers and other staff members.

Missing persons

There is no provision in the legislation for the creation of DNA profiles of missing person and their families. It is possible that this process occurs under the ambit of the consensual DNA sampling provisions; if so, this raises the additional concern that missing persons and their families have their DNA profiles stored in the criminal investigation database.

Sharing with overseas partners

It is understood that in 2013, New Zealand signed a "Pruem-like" sharing agreement (named after the EU's Pruem data-sharing agreement) with the US, to allow each country legal access to the other's fingerprint database under specified conditions, for automated searching. The agreement will also allow each country legal access to the other's DNA database, “if permissible under the national law of both Parties and on the basis of reciprocity”. There does not currently appear to be a lawful basis in the Act for the US authorities to access the DNA databank.