American Society of Law Medicine & Ethics Report:

The Non-Forensic Use of Biological Samples Taken for Forensic Purposes: An International Perspective

Prepared for ASLME by:
Christopher H. Asplen, Esquire
Smith Alling Lane

Introduction

The regulation and monitoring of database samples taken for forensic purposes can be understood as a spectrum of law-making activity ranging from mandates to destroy forensic samples, to a complex combination of criminal and general privacy laws, to a complete absence of statutory or regulatory guidance. While issues such as who should be included in a database, how long profiles should be retained, and what searches can be conducted, are often clearly established in specific legislative language, the uses to which samples can be put subsequent to a usable database profile being developed is rarely so specifically regulated. Except for the small minority of countries that require the relatively expeditious destruction of samples once profiling has been performed and checked, countries generally fail to identify what uses may or may not be made of biological material. Given the potential uses, both appropriate or not, legal and illegal, it is surprising how little attention has been paid, globally, to the issue of the non-forensic uses of forensic samples. This paper will examine how various countries outside the United States have addressed, or failed to address, the issue of permissible uses of biological samples taken for forensic purposes. Nations considered include the United Kingdom, member countries of the European Union, Australia, New Zealand, and Japan. We selected these nations because of their relatively sophisticated forensic DNA database system and regulatory regime.

Understanding the Forensic Context

The application of DNA technology in the forensic context is responsible for an epochal change in the dynamics of criminal justice systems throughout the world. Both in process and in result, judicial and investigative systems are different. As the single most tested and validated scientific evidence ever presented in court, it has changed how the judicial and investigative systems consider and rely on scientific evidence. Forensic DNA analysis has changed the way judicial bodies examine the validity of scientific evidence. Fact finders are no longer impressed by the presentation of DNA evidence but rather are critical of its absence. This often occurs regardless of the true relevance of DNA to any given case. It has changed the way prosecutors approach both the investigation and the prosecution of cases and it has changed the way defense attorneys defend them. The expectation of fact finders regarding DNA must be addressed even in its absence.

From an investigative standpoint, law enforcement is only *beginning* to recognize the true potential of the technology. Initially, DNA was simply a better tool for police and prosecutors. Once investigators had identified a suspect through traditional investigative techniques, DNA technology could confirm (or deny) the identity of the perpetrator. Once DNA's admissibility was established, prosecutors were presented with the most impressive evidence available.

However, it was not until DNA technology was combined with databasing technology that DNA began to change the actual investigative dynamic. No longer was the traditional investigative process of taking witness statements and descriptions, tracking down alibi witnesses and examining other (often less useful) forensic evidence a pre-requisite to realizing DNA's incriminating power. With the ability to take a DNA profile from crime scene evidence and compare it to a set of profiles from individuals

already deemed by society capable of committing crime, police can simply use the power of the technology rather than relying on others forms of evidence.

This is a global dynamic. A testament to the crime solving power of DNA technology is the fact that *no government, having established a forensic DNA Database, has ever reversed course and reduced the scope of inclusion for that database*. Expansion of criteria for database inclusion has been the only direction taken by jurisdictions in amending or updating their forensic DNA laws.

However, the passage of laws allowing the government to take a biological sample from an individual, produce a DNA profile and then store that information in a readily accessible database has been gradual and incremental. In recognition of the uniquely sensitive nature of an individual's genetic make up, countries throughout the world have approached offender databasing, in most instances, slowly and cautiously. Many began the process of databasing by limiting the application of DNA databases to those convicted of certain offenses. Typically, those qualifying offenses were of the most serious and heinous nature. This dynamic usually resulted from a public policy concern about the use of sensitive genetic information in law enforcement. Public policy concern is now less in evidence. A number of jurisdictions now permit DNA samples to be collected from suspects. In general, European nations now allow DNA samples to be taken from suspects and entered into a DNA database. This differs from the custom in most, but not all, US states that require a conviction before a DNA sample can be taken for profiling and inclusion in the DNA database. As DNA samples are taken from a broader segment of society, the question of appropriate legislative safeguards for retention and, in particular, the permissible uses of such identifiable genetic samples becomes more pressing.

Public Policy Cost - Benefit Analysis

The public policy debate upon which these databasing laws were founded involved a cost-benefit analysis - the cost of giving the government power and control over individuals' genetic information versus the crime solving (and thus crime prevention) benefit of DNA databases. In the US, as well as in much of the rest of the world, law enforcement's advocacy for authority to collect this type of sensitive information was based on two arguments. First, the crime solving potential of DNA technology combined with computer databasing technology is extensive. Second, the genetic information being gathered and retained by the government was extremely limited in scope. In fact, the argument went, one of the significant considerations for the selection of databasing loci (utilized in CODIS or other systems) was the "non-coding" nature of the sequences considered. Thus, the government could do little more with the selected loci than search a database because the loci were of little use for other purposes. The database loci could not enable the government to determine genetic predisposition to diseases, paternity, predisposition to behavioral traits, etc. Based on the loci selected and on the current state of knowledge, either in the US, UK or elsewhere, these propositions were, and remain, true.

The argument concerning the "safety" of the Combined DNA Index System (CODIS) and the non-coding nature of the developed profiles, however, was only really valid for the digitalized profiles themselves. The argument failed (and still fails) to address the practice of retaining DNA samples taken for profiling. It is true that the uses

to which profiles can be put – either in accordance with law or in violation thereof – are extremely limited. The same, however, cannot be said of the biological material from which the profiles are generated. The uses to which the biological samples themselves can be put, absent significant regulation and monitoring, are extensive, and will likely become more so as new technologies are developed. With this background, the following sections outline the laws in the countries set out above and examine any provisions that regulate the non-forensic use of retained DNA samples taken for forensic purposes.

England and Wales

Overview of Development and Current Regulation

The use of forensic DNA databases in England and Wales is rightly considered the most effective anywhere in the world. From the solving of the ground-breaking case of Colin Pitchfork, DNA has been utilized as an investigative tool, not simply a better piece of evidence available to the prosecution in court. Thus, it is instructive to describe in some detail the development of current policy with regard to sample retention and potential non-forensic uses.

The National DNA Database was established in 1995 following the recommendation of the influential Royal Commission on Criminal Justice. The Royal Commission was established in 1991, in response to an erosion of public confidence in the UK criminal justice system. One source of that concern was the quashed convictions of the "Birmingham Six,"[1] the exonerations of whom were handed down the same day that the Commission was announced. When the Commission published its recommendations in 1993, it stated that "there should be clear legislative provision for the more extensive storage of DNA samples or data both for the purpose of identifying offenders…."[2]

Since its establishment in 1995, the National DNA Database has received consistent legislative expansion and financial support from the UK Government. Through a series of Parliamentary Acts from 1993 through 2003, police have seen their ability to reap the benefits of DNA technology steadily enhanced. In 1993, the House of Lords' Select Committee on Science and Technology recommended that - given a lack of legislative authority for the collection, retention and use of biological samples - the government clarify the laws empowering police to use such evidence. In 1994, the Home Office commissioned the Metropolitan Police Forensic Science Laboratory to perform a pilot study to examine the use of DNA in the context a forensic database. As a result of this "Met" study, the Home Office decided to pursue the creation of a forensic DNA database.

The first Parliamentary Act establishing the authority to create a criminal DNA database was the 1994 Criminal Justice and Public Order Act (CJPOA).[3] "The central and most far reaching, aspect of the CJPOA was the framework it created for the police administration of DNA sample collection necessary for profiling.[4] The CJPOA broadened the scope of suspects from who samples could be taken to those charged with any 'recordable offense.'" This represented significant expansion beyond the "serious arrestable offence" scope of offenders that was established by the 1984 Police and Criminal Evidence Act (PACE).[5]

Importantly though, the CJPOA also amended the types of biological samples that could be collected from suspects. "Through a reclassification of the sample types defined

as 'intimate' and 'non-intimate,' the CJPOA redefined PACE to incorporate saliva and mouth samples in that category of non-intimate body samples which can be taken without consent and, crucially, by the police themselves."[6] In other words, while the 1984 PACE Act allowed for the collection of evidence from suspects, that evidence was limited to non-intimate samples, i.e.: fingerprints. DNA sample collection, absent the change of language to include saliva and mouth samples as "non-intimate" would have left DNA, for all practical purposes, un-collectable. Further, by facilitating the use of buccal swabs for sample collection, the CJPOA simplified sample collection and reduced cost significantly.

While the CJPOA called for the expungement of profiles of individuals who were not ultimately convicted, periodic problems with database administration ultimately led to a number of cases in which suspects were identified by samples which were retained in the system but should have been removed. This led to a number of court cases and a decision from the House of Lords addressing the legality of such identifications. Ultimately, the issue became one of discretion for the court.[7]

To address these public policy and legal issues, the House of Lords passed the 2001 Criminal Justice and Police Act (CJPA) which "…can be seen as a direct outcome of the problems of admissibility and retention."[8] The Act provides for the indefinite retention of DNA profiles on the NDNAD even if suspects are not convicted or "cautioned" for a crime.[9] It also allows for the indefinite retention of profiles and biological samples given voluntarily with written consent, such as through mass screenings. Thus, the 2001 CJPA allows for the collection and retention of biological samples and DNA profiles for anyone who becomes a suspect during the course of a police investigation.[10]

Despite the multiple legislative initiatives creating the most extensive databasing system in the world, and despite the stated desire to address the issue of sample storage, the extent to which such storage is considered is limited to whether or not samples can be stored. Legislation is devoid of language addressing any legal and appropriate "other" potential uses for these samples – including an outright prohibition against other uses.

Research Undertaken by the FFS Using Genetic Samples

The Forensic Science Service is the official custodian of both data and biological material in the UK and Wales. If research is to be performed, permission is requested of the National DNA Board (NDNAB).[11] Five research proposals have been submitted to the NDNAD Board for consideration prior to 1995. Of these, two were approved, two were rejected and, as of March 2004, a decision was still pending on the fifth. The two successful projects related to identifying suspects via their ethnic or family backgrounds and both were conducted by the FSS. Neither project sought the informed consent of participants. However, the database itself has been used in an attempt to link DNA profiles with ethnicity. The NDNAD has not been used for research related to behavioral genetics**.** Because the details of the requests and projects are not made publicly available, it remains unclear whether or not the DNA samples linked to the database have been used in any research.

Table of all Requests for NDNAD Based Research between 1995 and 2005.[12]

From	Received	Agreed
External research request from universities, etc.	6	1
Police operational requests relating to specific investigations, including familial searching	4	2
Requests to assist forensic providers for R&D papers, for future use in cases not specific investigations	11	6
Database improvements	1	1

The Netherlands

The Dutch approach to forensic DNA databasing is unique in several respects. On one hand, it is the only country which specifically, legislatively allows for the analysis of "physical characteristics" on DNA samples. While other countries such as the United States and the United Kingdom have begun testing samples for characteristics such as red hair and for "bio-geographical diversity," only the Netherlands has approached the subject in a direct and legislative context.

While addressing physical characteristics testing so directly, however, only recently has the Dutch government passed legislation allowing for the analysis and database entry of convicted offender sample profiles. Under the previous law, law enforcement was restricted to utilizing only samples from suspects and only in those cases in which DNA was relevant to the investigation.

What is particularly unique to the Dutch system however is the creation of the Privacy Audit Framework under the new Dutch Data Protection Act (WBP). It is derived from and designed specifically to comply with the European Data Protection Directive 95/46/EG, described more fully in the following section. Replacing the previous Dutch Data Protection Act of 1989, the new Act sets requirements on the entire processing chain, including collecting, recording, storing, altering, linking and consulting of personal data as well as disclosing personal data to third parties and the erasure or destruction of personal data. The previous Act regulated only the requirements with regard to "personal data registrations." Responsible for monitoring the correct observance of the law is the National Data Protection Board. The Board has specifically designated cell material as "personal data" and as such, any use, research etc. of **forensic** samples must comply with the WBP.

European Union (EU)

Member countries of the European Union need not only comply with the statutes, rules and regulations of their own government, but in many instances with the laws, resolutions and directives set forth by the government in Brussels. In a very complex relationship, the nature and extent to which EU laws enter into the workings of any given country vary significantly with the nature of the subject matter being regulated. For example, EU regulations regarding commerce and the travel of EU citizens across boarders are authoritatively controlled by European-wide legislative initiatives. There are however many areas in which the EU has little or no authority to regulate within the borders of individual member countries.

Originally, criminal justice issues were left relatively untouched by Brussels. Individual States' criminal justice systems maintained complete sovereignty. However, with the advent of non-regulated cross boarder traffic as well the rise of incidents of international terrorism, the European Commission has recognized the need to more closely coordinate its efforts in various areas.

EU Directive 95/46/EC

The EU Directive 95/46/EC on Data Protection took effect in October 1998.[13] Passed by the European Parliament and the European Council on 24 October 1995, the directive focuses on the protection of individuals with regard to the processing of personal data and the free movement of such data.[14] Currently, the EU member states of Belgium, Czech Republic, Denmark, Germany, Estonia, Greece, Spain, France, Ireland, Italy, Luxembourg, Hungary, Malta, the Netherlands, Austria, Poland, Cyprus, Latvia, Lithuania, Portugal, Slovenia, Slovakia, Finland, Sweden, and the United Kingdom have all adopted a version of Directive 95/46/EC to regulate the processing of personal data.[15]

Several definitions and scope parameters set forth in Articles 2 and 3 of Directive 95/46/EC help to define its potential applicability to DNA database samples. Article 2, Section (a) of the Directive defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject')."[16] In the same Article and Section, the Directive subsequently defines an "identifiable person" as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[17] Moreover, according to Article 3, the Directive applies to "the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."[18] Article 3 however, also articulates that *the Directive does not apply to the processing of personal data when such processing operations involve the activities of a State in areas of criminal law.*[19]

These definitions and scope parameters support the notion that DNA samples, which are collected from individuals for use in DNA databases to generate criminal profiles, are "personal data" relating to "identifiable persons," but that they are not within the scope of the Directive because they are collected in the course of criminal procedure. As such, when DNA samples are obtained from suspects and convicted offenders, and used solely for forensic purposes in criminal investigations, it is likely that the Directive does not govern the processing and movement of these DNA samples and profiles.

However, a different outcome may result when DNA samples are retained beyond the life of the criminal investigation and are subsequently used for non-forensic purposes.

The time and manner of such non-forensic use should disqualify the DNA sample from falling under the Article 3 exception and thereby bring it back into the scope of the Directive. If retained DNA samples are used for purposes other than those related to criminal forensics, then the Directive will apply to govern the processing and movement of such DNA samples.

Keeping such DNA samples in mind, numerous provisions of the Directive are worth noting for their apparent applicability:

Article 1, Section 1
In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.[20]

Article 7
Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).[21]

Article 8, Section 1
Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.[22]

Article 8, Section 3
Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.[23]

Article 8, Section 5
Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards

are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority. Member States may provide that data relating to administrative sanctions or judgments in civil cases shall also be processed under the control of official authority.[24]

Article 12
Member States shall guarantee every data subject right to obtain from the controller:
(a) without constraint at reasonable intervals and without excessive delay or expense:
(1) confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, (2) communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, (3) knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

Article 13, Section 1
Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defense;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.[25]

Article 13, Section 2
Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.[26]

Article 17, Section 1
Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.[27]

Article 20, Section 1
Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.[28]

Cooperative Agreements among EU Members
As evidence of growing cooperation among the EU members, the European Commission launched a five-year Action Plan for Freedom, Justice and Security on May 10, 2005.[29] This Plan advocates the increase of cross-border cooperation, new information systems, electronic networks, and data sharing among EU members. Initially, four EU members (Belgium, France, Germany, and Spain) reached an agreement to allow for the exchange of their criminal records via electronic means. This exchange system is expected to fully function by the end of 2005 and is open to cooperation by all EU Member States and the European Commission.

On May 27, 2005, seven members of the EU, namely Belgium, Germany, Spain, France, the Netherlands, Luxembourg, and Austria, signed a landmark agreement.[30] This document, the "Schengen III Treaty," allows for increased security cooperation and data-sharing among EU members in the criminal justice arena.[31] The Schengen III Treaty allows police and other appropriate authorities to have automatic access, via "contact points," to the DNA databases of the other signatory countries in order to pursue criminal offenses. Such access will help to determine whether a DNA profile, generated from a crime scene, has already been registered in another country's DNA database. However, the agreement states that a criminal suspect's identity will only be revealed once a formal legal request for his identity has been issued.

Consistent with most legislation addressing databases, the Schengen Treaty does not explicitly mention non-forensic uses of the DNA samples that are originally collected to generate forensic profiles. In spite of the careful crafting of various aspects of the agreement and the privacy concerns expressed in each of the member countries, once again, this issue is left unaddressed.

EU Member Regulations on Sample Retention and Destruction
The clearest and most definitive policy or regulation regarding the permissible non-forensic uses of forensic samples comes in the context of required sample destruction. The destruction of database samples subsequent to a usable profile being developed simply eliminates the potential of further non-forensic uses. Despite that, only Germany[32] and Belgium[33] require that DNA samples are destroyed as soon as the criminal profile resulting from the DNA database is developed and finalized. In other member countries, a diversity of approaches is taken to the length of sample retention and triggers for sample destruction.

With the noted exceptions of Germany and Belgium, EU member states allow for the retention of DNA samples beyond their use in developing DNA databases to generate criminal profiles. For example, the United Kingdom's Human Tissue Act of 2004

permits the collection and retention of DNA tissue samples and the processing of DNA profiles for "excepted purposes," including: to prevent and detect crimes, to diagnose and treat medical conditions, to use during the conduct of prosecution, to meet goals of national security, and to implement court orders.[34]

Unlike the United States, most other countries, and indeed the majority of Europe, routinely obtain DNA samples from suspects. Most offender databases are developed around a suspect profile database, rather than a convicted offender database. As such, there are numerous different time tables and criteria which trigger sample destruction. Oftentimes sample destruction is approached differently depending on whether or not the sample is taken from a suspect or from a convicted offender. The time requirement for the destruction of samples ranges from immediately after a usable DNA profile is developed to never.

Sample Destruction Policies[35]

Country	Convicted Offenders	Suspects
Austria	Sample is retained	Suspect must apply for profile removal and sample destruction if acquitted
Belgium	Sample must be destroyed immediately after profile is obtained.	Sample must be destroyed once informed no counter-expertise has been requested.
Czech Rep.	No specific legislative provision made for sample retention or Destruction Sample fate usually follows profile Fate	No specific legislative provision made for sample retention or Destruction Sample fate usually follows profile fate (No suspect database)
Estonia (Planned legislation)	N/A	N/A
Finland	Sample destruction is tied to profile removal: Sample must be destroyed and profile removed one year from the	Sample destruction is tied to profile removal: Sample must be destroyed and profile removed one year from the
France	Samples retained for 40 years after sentence or until individual reaches age limit (80 years old).	Suspect sample is returned to the magistrate or police officer in charge and is kept like any other piece of evidence. If the suspect is convicted, sample is forwarded to Gendarmerie storage facility for preservation (SCPPB)
Country	**Convicted Offenders**	**Suspects**

Germany	All reference samples must be destroyed after DNA analysis.	All reference samples must be destroyed after DNA analysis. However, samples taken for casework purposes (expert report) have to be kept until the criminal proceedings have been terminated by a final decision.
Greece	N/A	If a suspect is run against the database, sample must be destroyed within 10 days
Hungary	May retain biological reference sample as long as the right exists to maintain profile in database	May retain biological reference sample as long as the right exists to maintain profile in database
Italy (No legislation pending)	N/A	Samples are stored
Rep. of Ireland	N/A	N/A
Netherlands	Biological sample is stored as long as the profile itself. Profile storage times vary. 20 years if convicted of crime with potential 4 – 6 year sentence. 30 years if convicted of crime with potential sentence of more than 6 years.	If suspect is convicted, sample is stored as long as profile is kept. Profile storage times vary: 20 years if convicted of crime with potential 4 - 6 year sentence. 30 years if convicted of crime with potential sentence of more than 6 years. If suspect is acquitted, profile must be removed.
Norway	Samples must be destroyed when profile is entered into the database	Sample must be destroyed when profile is entered into the database
Northern Ireland	No legal requirement to destroy samples.	No legal requirement to destroy samples.
		Local force direct the destruction Of samples in some circumstances following acquittal/termination of proceedings
Portugal	N/A (Current database contains only crime scene stains)	N/A (Current database contains only crime scene stains)
Poland (Legislation pending)	Will require sample retention	Will require sample retention
Scotland	Samples are retained indefinitely	Samples are retained indefinitely
Spain (unapproved draft guidelines only)	Once time for possible counter - analysis has expired, samples will be destroyed with judicial authorization	Once time for possible counter - analysis has expired, samples will be destroyed with judicial authorization
Sweden	Saved for two years If offender is dead, saved for 25 yrs	Saved for two years If offender is dead, saved for 25 yrs
Country	**Convicted Offenders**	**Suspects**

Switzerland	All samples and the attached DNA must be destroyed within three months from entry of the profile into the database or as soon as the sample is no longer needed for comparison purposes.	All samples and attached DNA must be destroyed within three months from entry of the profile into the database or as soon as the sample is no longer needed for comparison purposes.
United Kingdom	Law allows for retention of all legally obtained samples indefinitely.	Law allows for retention of all legally obtained samples (even if acquitted).

Australia

Australia is a democratic, federal-state system consisting of 6 states and 2 territories. However, despite the relatively few number of states and territories, Australia has experienced a significant lack of coordination between those jurisdictional entities when it comes to forensic DNA applications. Rather than developing the legal authority to share forensic DNA profiles across jurisdictional borders by way of the creation of a national sharing system (similar to the National DNA Database System), States and Territories in Australia share DNA data through a series of bi-lateral agreements between each other. Not surprisingly, there is also significant lack of coordination regarding the non-forensic use of database samples.

In 1989, the Australian Federal Government, as well as several States and Territories, began to develop regulatory standards for DNA collection and handling procedures.[36] By 1990, five Australian states and territories had undertaken DNA analysis. In 1992, the National Institute of Forensic Science (NIFS) began its operations in the area of DNA databasing.[37] The NIFS strives to develop national standards of quality control and accreditation of forensic laboratories throughout Australia.[38] However, its role is to sponsor research, act as a clearing house of information and develop quality assurance programs. Compliance with NIFS' standards is voluntary and it offers no policy advice on sample retention.

The Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General published the Model Forensic Procedures Bill (Model Bill) in May 1999 to act as a guide for the Australian territories to develop or enhance their DNA legislation.[39] As it is a "Procedures" bill, it does not address who should be included in the database, other than to provide for procedures for the sampling of both suspects and convicted offenders. There is no further recommendation as to subclasses of each category. Also, non-forensic uses of biological material are not addressed directly. However, the issue of sample destruction, under various collection scenarios, is addressed rather extensively.

Division 10 Destruction of forensic material

75 Destruction of certain forensic material obtained by court order

(1) If an interim order for the carrying out of a forensic procedure made under section 26 is disallowed after the forensic procedure is carried out, the investigating police officer must ensure that:

(a) any forensic material obtained as a result of the carrying out of the procedure is destroyed as soon as practicable after the disallowance, and

(b) a copy of the results of any analysis of the forensic material is

made available to the suspect.

(2) If an order for the carrying out of a forensic procedure made under section 68 (Regarding sampling of a child or incapable person) or for the retention of forensic material under section 69 specifies a period for which forensic material obtained as a result of the carrying out of the procedure may be retained, the forensic material is to be destroyed as soon as practicable after the end of the period.

76 Destruction of forensic material taken from offender after conviction Quashed

The police officer who obtained an order under section 62 for the carrying out of a forensic procedure on an offender whose conviction is quashed after the making of the order must ensure that any forensic material obtained as a result of the carrying out of the procedure is destroyed as soon as practicable after the conviction is quashed.

77 Destruction of forensic material after 12 months

(1) This section applies where forensic material has been taken from a suspect by a forensic procedure carried out under Division 3, 4 or 5.

(2) If:

(a) forensic material has been taken from a suspect, and

(b) a period of 12 months has elapsed since the forensic material was taken, and

(c) proceedings in respect of an offence to which the forensic material relates have not been instituted or have been discontinued,

the forensic material must be destroyed as soon as is practicable unless a warrant for apprehension of the suspect has been issued.

(3) If a warrant for the apprehension of the suspect is issued during the period of 12 months after forensic material is taken the forensic material must be destroyed as soon as practicable after:

(a) the warrant lapses, or

(b) a period of 12 months elapses after the suspect is apprehended.

(4) If forensic material has been taken from a person who is a suspect and:

(a) the person is found to have committed an offence to which the forensic material relates but no conviction is recorded, or

(b) the person is acquitted of such an offence and:

(i) no appeal is lodged against the acquittal, or

(ii) an appeal is lodged against the acquittal and the acquittal is confirmed or the appeal is withdrawn,

the forensic material must be destroyed as soon as practicable unless an investigation into, or a proceeding against the person for, another offence to which the forensic material relates is pending.

(5) A magistrate may, on application by a police officer or the Director of Prosecutions *[an appropriate reference should be inserted in each jurisdiction to ensure that this covers any person prosecuting a relevant offence]*, extend for a period not exceeding 12 months the period for which forensic material may be retained under this section, if the magistrate is satisfied there are special reasons for doing so.

(6) A magistrate to whom an application is made under subsection (5) is not to extend the period unless:
(a) the person from whom the forensic material was taken has been notified by the applicant for the extension that the application has been made, and
(b) the person or his or her legal representative or interview friend (if any) has been given an opportunity to speak to or make a submission to the magistrate concerning the extension.
(7) An extension in relation to particular forensic material may be given on more than one occasion.
(8) The magistrate is to ensure that the responsible person in relation to the DNA database system is notified of any extension given under this section.

78 Destruction of forensic material where related evidence is inadmissible
If a court finds that evidence described in section 70 (4) relating to a forensic procedure is inadmissible under section 70, the Commissioner of Police must, as soon as practicable, ensure that any forensic material taken from the suspect by that forensic procedure is destroyed.

97 Taking, retention and use of forensic material
(1) **Taking, retention and use authorized by laws of other jurisdictions**
Nothing in this Part affects the taking, retention or use of forensic material, or information obtained from forensic material, if the taking, retention or use of the material is authorized by or under another law of the State *[or Territory]* or a law of the Commonwealth.
(2) Forensic material, or information obtained from it, that was taken in accordance with the law of another State or a Territory may be retained or used in this State *[or Territory]* for investigative, evidentiary or statistical purposes even if its retention or use would, but for this subsection, constitute a breach of, or failure to comply with, any provision of this Part relating to the carrying out of forensic procedures.
(3) **Use and retention of forensic material taken before commencement of subsection**
Forensic material, or information obtained from it, that is taken in accordance with the law of this or another State or a Territory, as in force immediately before the commencement of this subsection, may be retained or used in this State *[or Territory]* for investigative, evidentiary or statistical purposes even if its retention or use would, but for this subsection, constitute a breach of, or failure to comply with, any provision of this Part relating to the carrying out of forensic procedures.

The Commonwealth, New South Wales, and the Australian Capital Territory closely follow the Model Bill, with a few variations.[40] Tasmania has followed the Model

Bill in some respects, but with more variations.[41] Victoria and South Australia have recently amended their legislation to bring their laws into closer conformity with the Model Bill, even though some significant variations remain.[42] Western Australia implemented legislation that conforms in some respects with the Model Bill.[43] On the other hand, the Northern Territory has not followed the Model Bill at all.[44] In the Northern territory, because the police do not classify DNA samples as "intimate," they are able to secure such samples without obtaining consent or even a court order.[45] Queensland does not follow the Model Bill either, although it has indicated a willingness to amend its legislation to facilitate participation in a national DNA database system.[46] The Privacy Commissioner (NSW) however has some difficulties with the approach taken in the Model Bill:

> "As long as a retained sample exists there is the possibility of re-identifying the person it comes from through comparison with another sample from the same person. The Model Bill recognizes this to the extent that it makes it an offence to analyze samples that have been approved for destruction. Sections 65 and 66 [Now ss.70 and 71] which prevent the admission of destroyed samples into evidence. These safeguards would not necessarily prevent the reuse or threatened reuse of a sample to pressure a person into making an admission. The Bill should explicitly rule out the reuse of samples which have been anonymised in accordance with the requirements for destruction."[47]

On July 1, 2000, the CrimTrac Agency was established in Australia. This law enforcement agency powers a national DNA database in Australia entitled the National Criminal Investigation DNA Database (NCIDD).[48] While participation in the NCIDD system is voluntary and pursuant to memorandum of understanding between CrimTrac and the individual jurisdictions, it gives police access to DNA profiles in order to help them solve crimes.[49] Currently, agreements have been signed with Queensland, Victoria, Commonwealth, New South Wales, Australian Capital Territory and eastern Territory. CrimTrac hosts a database of DNA profiles that are used for inter-jurisdictional and intra-jurisdictional matching purposes. However, as of June 2005, the NCIDD held only 152, 594 profiles from crime scenes, offenders, suspects, volunteers and missing persons. Moreover, CrimTrac neither collects nor stores the DNA samples themselves.

In 2003, the Australian Law Reform Commission (ALRC) produced a report entitled "Essentially Yours: The Protection of Human Genetic Information in Australia" (ALRC Report 96).[50] Section 8 addresses the issue of privacy of genetic samples. Section 13 defines and discusses human genetic research.[51] Section 18 describes the regulation of human genetic research databases.[52] Sections 25-38 address various uses for genetic information in the following arenas: insurance, employment, parentage testing, kinship and identity, immigration, and sports.[53] Section 39 of ALRC Report 96 details the forensic uses of genetic information.[54] Specifically, this section addresses the development of the aforementioned Model Bill, which provides rules for the regulation of DNA database systems.[55]

In 2005, legislation was passed by the Federal Parliament that enables Australia's national forensic DNA database system to be used in efforts to identify disaster victims within Australia. This is landmark legislation for the use of DNA samples beyond the

realm of criminal investigations, and would allow the national DNA database system to be used for the purpose of identifying missing or dead persons following a domestic mass casualty incident.[56] In addition, stored DNA samples may be used in the judicial system during post-conviction review.[57]

New Zealand

New Zealand was the second country in the world to legislate the creation of a national forensic DNA database. It is also the only country in the world in which the custodian of the database is a private entity, The Institute of Environmental Science and Research. There are no allowable non-forensic uses of samples collected for the database.

The issue of DNA testing first surfaced in New Zealand in 1978, when the New Zealand Criminal Law Reform Committee (NZCLRC) published a controversial report entitled "Bodily Examination and Samples as a Means of Identification."[58] After lying dormant for years, the DNA testing issue resurfaced in the late 1980s, when a private bill was introduced that proposed many of the same recommendations as the earlier NZCLRC report.[59] A few years later, New Zealand's Minister of Justice proclaimed governmental support for DNA testing and a national DNA data bank.[60]

In 1995, the Criminal Investigations (Blood Samples) Act was passed in New Zealand.[61] This Act allowed for the taking of DNA samples from innocent volunteers, criminal suspects, and convicted criminals (guilty of certain offenses), and all of these samples are stored in a national databank.[62] Beginning in 1998, the data bank was used to search for comparisons between the individual DNA profiles and unsolved crime scene profiles.[63] More specifically, the samples in the database were matched against DNA profiles obtained from unsolved crimes in an attempt to identify any individual that could be linked to an offense via biological material left at the crime scene.[64]

Significantly, the original Act was amended in 2003 to accommodate scientific advances in forensic DNA technology, and it is now entitled the Criminal Investigations (Bodily Samples) Act of 1995.[65] This new Act allows DNA samples taken from buccal (mouth) swabs to be included on the data bank, in addition to DNA samples taken from blood.[66]

In New Zealand samples obtained from individuals cannot be used for any other purpose other than to obtain a profile to place onto the National DNA Data bank. The samples, extracted DNA and amplified DNA products must be destroyed after the DNA profile has been obtained. The specific text from the Criminal Investigations (Bodily Samples) Act 1995 is:

> Part III, s28: Access to and use of bodily samples held for DNA profile data bank purposes-
>
> No person may have access to, and no person may use, any bodily sample-
>
> (a) To which section 60(2) of this Act applies; or
>
> (b) Taken from any person pursuant to this Part of this Act- except for the purpose of deriving from that sample a DNA profile for storage on a DNA profile data bank.

(Section 60 relates directly to the disposal of the samples).

Currently, the DNA data bank holds over 16,000 individual DNA profiles, with approximately 400 new profiles being added each month.[67] The database also holds over 1,900 crime scene profiles, with approximately 120 more profiles being added each month.[68] The Institute of Environmental Science and Research administers the national DNA data bank on behalf of the New Zealand police.[69]

Japan[70]

Full-scale DNA analysis was introduced in Japan in 1989. The Shimotsuma branch of the Mito District Court was the first to acknowledge the credibility of DNA analysis in a rape trial in 1992. Later, in 2000, Japan's Supreme Court ruled for the first time that DNA tests were scientifically trustworthy. In August of 2003, each of Japan's 47 police prefectures (local police districts) received a precision DNA analyzer.

In December 2004, Japan's National Police Agency (NPA) created a national database of DNA evidence collected from crime scenes. The NPA also compiled guidelines for using the database and distributed it to Japan's 47 prefectural police offices. Under the guidelines, each prefectural office's criminal investigation laboratory sends the DNA samples that are collected from crime scenes to the agency's scientific examiners. If the examiners find matching information in the database, they issue a notice to all laboratories concerned. The database is strictly controlled by the NPA's Criminal Identification Division and can only be accessed by a limited number of people at the NPA. In accordance with instructions the NPA issued to police across Japan in July of 2003, however, coding sequences are not used.

Structurally, Japan's National Police Agency (NPA) oversees the country's DNA databases. Within the NPA, the Criminal Investigation Bureau's Criminal Identification Division maintains Japan's national DNA database of crime scene samples. Also under the National Police Agency, the National Research Institute of Police Science's Department of First Forensic Science is responsible for laboratory research and casework in the field of forensic biology. This Department's Fourth Biology Section handles examinations, research and case work concerning forensic DNA analysis of biological samples from crime scenes. As of this writing, the National Police Agency has convened a six member "panel of experts," on law and medicine who have been charged with studying the questions around which the country's DNA database should be implemented. The recommendations of this panel may impact developments in this area, and will be worth studying when they become available.

On June 1st 2005, upon the decision of the panel of experts the NPA began compiling a new database of DNA information on criminal suspects for use in police investigations. The new database will be put on strict control and only NPA personnel in charge of the database will be allowed to access it. When it is completed in August, the database will be linked with the existing database of crime scene evidence and allow investigators to conduct online cross-referencing of DNA profiles obtained from evidence such as blood, hair and body fluids to identify a suspect. However, the agency has deferred requiring the collection of DNA from convicted individuals or arrested suspects for reasons of privacy.

In the past, Japanese police have taken DNA samples from suspects in heinous crimes, such as murder and rape, when samples were needed to match DNA evidence

found at the crime scene. However, in these cases, police obtained court-issued warrants to take the DNA samples. In their decision on June 1st, the NPA decided not to set limits on the types of crimes requiring DNA samples from suspects. Instead, at their discretion, Japanese police may continue to ask for court-issued warrants to take DNA samples when such samples are considered vital to an investigation. While the NPA has the authority to take a DNA sample from a suspect with a court-issued warrant, the NPA does not believe that current laws allow them to take samples from suspects without a warrant.

The NPA's panel of experts plans to consider the necessity of developing legislative measures to assist with the effectiveness of the database. These measures are likely to include an expansion of the authority under which DNA can be collected. However, at the same time, the panel also plans to review potential problems concerning ethics and privacy rights, such as how the DNA of suspects would be handled if they are proven innocent.

As no legislation currently exists regarding the workings of the national database, there is no legislative direction regarding the non-forensic use of database samples. The rules and regulations set forth buy the National Police Agency however, seem to be rather restrictive. Given the self-imposed restrictions under the current database procedures, it is likely that non-forensic uses would be prohibited.

References

1. The six were arrested in 1974. They had left Birmingham shortly before the bombs exploded in two city centre pubs in the bloodiest ever IRA attack. Twenty-one people were killed, more than 160 injured. The men claimed in court they had confessed only after being beaten by police. A new inquiry by Devon and Cornwall Police into the original inquiry uncovered irregularities in the police case against the Six. New scientific tests show statements made by the Birmingham Six were altered at a later date. Scientists also admitted in court that forensic tests which were originally said to confirm two of the six had been handling explosives could have produced the same results from handling cigarettes.

2. P. Roberts, C. Willmore, *The Royal Commission on Criminal Justice: The Role of Forensic Science Evidence in Criminal Proceedings* (London: Crown Copyright, 1993).

3. There is no law actually establishing the National DNA Database. Rather the law allows for the collection and retention of the samples for police use. The model for the sample collection was the collection of fingerprints. This fact, more than any other contributed to the creation of the database as being populated by suspects rather than convicted offenders.

4. P. Johnson, P. Martin and R. Williams, "Genetics and Forensics: Making the National DNA Database," submitted for publication to *Science Studies* (2003).

5. Police and Criminal Evidence Act.

6. P. Johnson, P. Martin, and R. Williams, *supra* note 4, at 12.

7. *Id.*

8. *Id.*

9. A caution is the formal disposal of a criminal case without the intervention of prosecutors or the courts. About a third of all criminal cases resulting in a criminal record are disposed of by a police caution rather than by conviction. Cautions are kept on record and can influence future prosecution and court decisions.

10. It should be noted that the changes were challenged as contravening the European Convention on Human Rights right to privacy. Ultimately, under a balancing test weighing public benefit against individual privacy, the European Convention issues were resolved in favor of benefits to public interest.

11. K. Staley, "Genewatch UK, The Police National DNA Database: Balancing Crime Detection Human Rights and Privacy," Briefing Number 31 (June, 2005), *at* <http://www.genewatch.org/HumanGen/Publications/Reports/NationalDNADatabase.pdf> (last visited March 9, 2006).

12. *Id.*

13. U.S. Department of Commerce, Safe Harbor Overview, *at* <http://www.export.gov/safeharbor/sh_overview.html>(last visited March 9, 2006).

14. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *available at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html> (last visited March 9, 2006).

15. See Europa, Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data, *at* <http://europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.htm > (last visited March 9, 2006).

16. See Directive 95/46/EC, *supra* note 14 *at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_28> (last visited March 9, 2006).

17. *Id.*

18. See Directive 95/46/EC, *supra* note 14 *at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_29> (last visited March 9, 2006).

19. *Id.* (Emphasis added).

20. See Directive 95/46/EC, *supra* note 14 *at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_27> (last visited March 9, 2006).

21. See Directive 95/46/EC, *supra* note 14 *at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_9> (last visited March 9, 2006).

22. See Directive 95/46/EC, *supra* note 14 *at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_11> (last visited March 9, 2006).

23. *Id.*

24. *Id.*

25. See Directive 95/46/EC, *supra* note 14 *at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_34> (last visited March 9, 2006).

26. *Id.*

27. See Directive 95/46/EC, *supra* note 14 *at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_37> (last visited March 9, 2006).

28. See Directive 95/46/EC, *supra* note 14 *at* <http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_40> (last visited March 9, 2006).

29. IDABC, *Data-Sharing and eNnetworks Central to EU's Freedom, Justice and Security Action Plan* (May 12, 2005) *at* <http://europa.eu.int/idabc/en/document/4332/330> (last visited March 9, 2006).

30. For a description of the Schengen III Treaty, see IDABC, “Seven EU Member States to Share Access to DNA and Fingerprint Databases” (May 30, 2005), *at* <http://europa.eu.int/idabc/en/document/4332/330> (last visited March 9, 2006).

31. *Id.*

32. The legal bases is included in German Federal Law: For the provision and examination of DNA samples: §§ 81a, 81e, 81f and 81g Rules of Legal Procedure (Strafprozessordnung); § 3 DNA-Identitätsfeststellungsgesetz ("act for the establishment of identity"). For the maintenance of the database: § 3 Identitätsfeststellungsgesetz and §§ 2, 7 and 8 Bundeskriminalamtgesetz (act for the Federal Criminal Investigation Office) Content of the German DNA-database: DNA-identification codes of known perpetrators and "latents" (samples secured as evidence at scenes of crimes).

33. Law of 22 March 1999 concerning the identification procedure by DNA analysis in penal matters. Publication: on May 20, 1999, Entry into force: March 30, 2002. Also to quote the Royal Decree of February 4, 2002 taken pursuant to this law, published and entered into force on March 30, 2002.

34. *Available at*, <http://www.opsi.gov.uk/acts/acts2004/40030--j.htm#sch4pt2> (last visited April 19, 2006).

35. Data was gathered pursuant to a survey taken of representatives to the European Network of Forensic Science Institutes (ENFSI) DNA Working Group, updated November 2005.

36. CrimTrac, *DNA History*, *at* <http://www.crimtrac.gov.au/dnahistory.htm> (last visited March 9, 2006).

37. *Id.*

38. *Id.*

39. A. Puri, "An International DNA Database: Balancing Hope, Privacy and Scientific Error," *Boston College International Comparative Law Review* 24 no. 2 (2001): 341-380, 372-374, *available at* <http://www.bc.edu/bc_org/avp/law/lwsch/journals/bciclr/24_2/05_TXT.htm> (last visited March 9, 2006).

40. Australian Law Reform Commission, *Forensic Uses of Genetic Information*, *at* <http://www.austlii.edu.au/au/other/alrc/publications/reports/96/39_Forensic_Uses_of_Genetic_Information.doc.html> (last visited, March 9, 2006).

41. *Id*.

42. *Id.*

43. *Id.*

44. *Id.*

45. See Puri, *supra* note 39, at 371.

46. See Australian Law Reform Commission, *supra* note 40.

47. Forensic Procedures Bill - DNA Database Provisions - Explanatory Notes, Model Criminal Code Officers Committee, February 2000, p. 6.

48. See CrimTrac, *About Us*, *at* <http://www.crimtrac.gov.au/aboutus.htm> (last visited March 9, 2006).

49. See Australian Law Reform Commission, *supra* note 42.

50. *Id.*

51. Australian Law Reform Commission, "Human Genetic Reserch," *at* <http://www.austlii.edu.au/au/other/alrc/publications/reports/96/13_Regulation_of_human_genetic_research.doc.html> (last visited March 9, 2006).

52. Australian Law Reform Commission, "Human Genetic Databases for Research," *at* <http://www.austlii.edu.au/au/other/alrc/publications/reports/96/18_Human_Genetic_Databases_for_Research.doc.html> (last visited March 9, 2006).

53. Australian Law Review Commission, "ALRC 96 Essentially Yours: The Protection of Human Genetic Information in Australia," *at* <http://www.austlii.edu.au/au/other/alrc/publications/reports/96/> (last visited March 9, 2006).

54. See Australian Law Reform Commission, *supra* note 40.

55. *Id.*

56. News-Medical.Net, "Legislation Introduced to Enable Australia's National DNA Database System to Be Used to Identify the Victims of Disasters within Australia," *at* <http://www.news-medical.net/?id=3967> (last visited April 6, 2006).

57. See Australian Law Reform Commission, *supra* note 52.

58. Puri, *supra* note 39 at 372.

59. *Id.*

60. *Id.* at 373.

61. *Id.*

62. *Id.*

63. *Id.*

64. ESR, "The New Zealand National DNA Databank," *at* <http://www.esr.cri.nz/competencies/forensicscience/dna/DNAdatabank.htm> (last visited April 6, 2006).

65. *Id.*

66. *Id.*

67. CrimTrac, "DNA Databases -The International Experience," *at* < http://www.crimtrac.gov.au/dnainternational.htm> (last visited April 6, 2006)

68. *Id.*

69. Austrialian Law Review Commission, *supra* note 40, *at* <http://www.austlii.edu.au/au/other/alrc/publications/reports/96/39_Forensic_Uses_of_Genetic_Information.doc.html#heading24>.

70. Information gathered from interviews with various members of the Japanese law enforcement and forensic community.