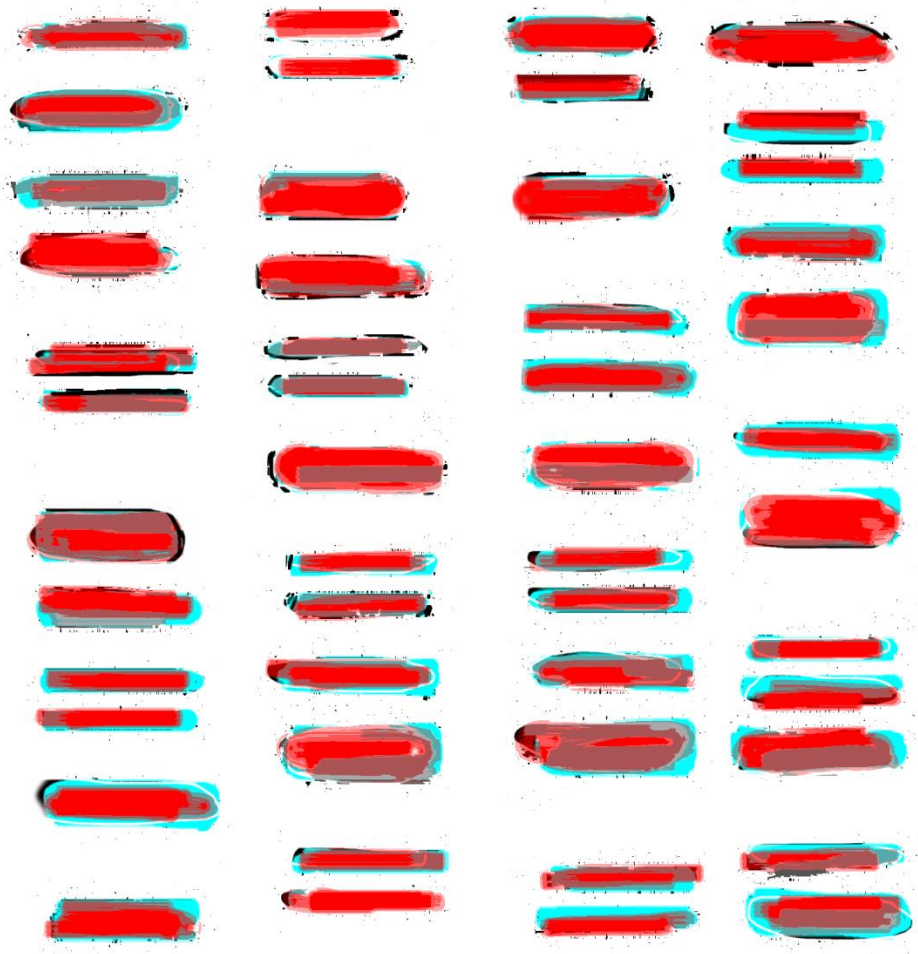
Establishing Best Practice for Forensic DNA Databases



FORENSIC GENETICS POLICY INITIATIVE

Setting Human Rights Standards For DNA Databases Worldwide

Establishing best practice for forensic DNA databases

September 2017

A report by the Forensic Genetics Policy Initiative:
http://dnapolicyinitiative.org/report/

The project

This report was developed by the Forensic Genetics Policy Initiative (http://dnapolicyinitiative.org/) using an innovative consultative approach. The final report reflects input from civil society groups around the world from a human rights perspective.

The project began as a result of civil society concerns about the lack of public input and debate regarding the development and expansion of forensic DNA databases around the world. The seven-year project has included extensive monitoring of press articles and legislation from 132 countries, visits to a number of countries with forensic DNA databases or developing new legislation (including UK, USA, China, India, Brazil, South Korea), and extensive discussion with civil society groups, policy makers, lawyers, forensic scientists and academics from many other countries.

The project has taken the innovative and unique approach of developing best practice international standards by engaging civil society in extensive discussion and debate. As a result, this report is the most wide-ranging and definitive analysis of human rights safeguards for forensic DNA databases that is available worldwide.

The final process of developing the report was led by a steering committee of twelve people from around the world, plus two observers acting as representatives of the United Nations Special Rapporteur on the right to privacy.

Steering Committee members:
Adeboye Adegoke (Nigeria)
Professor Ghanim Al-Najjar (Kuwait)
Tomaso Falchetta (UK/international). Privacy International.
Elonnai Hickok (India). Centre for Internet and Society.
Professor Sheldon Krimsky (USA). Council for Responsible Genetics.
Luiza Louzada (Brazil). Institute of Social Medicine at Rio de Janeiro State University IMS/UERJ.
Usha Ramanathan (India).
Arthit Suriyawongkul (Thailand).
Lee Tien/Jennifer Lynch (USA). Electronic Frontier Foundation.
Helen Wallace/Anthony Jackson (UK). GeneWatch UK.

As well as providing their own feedback, steering committee members facilitated further engagement with civil society, gathering input from their own stakeholders and further building consensus around the report.

The process also included a session at the 38th International Conference of Data Protection and Privacy Commissioners in Marrakesh, 18-22nd October 2016, hosted by the UN Special Rapporteur on Privacy, and another at RightsCon in Brussels, 29-31st March 2017, where the project presented draft best practice guidelines for feedback and discussion.

Additional organisations and individuals consulted included: Aaron Amankwaa (Ghana), Adedapo Adejumo (Nigeria), American Civil Liberties Union (USA), Chinmayi Arun (India), BC Civil Liberties Association (Canada), Pascal Borry (Belgium), Bytes for All (Pakistan), Center for Democracy in Science and Technology (South Korea), Manpreet Dhillon (India), Gen-ethisches Netzwerk (Germany), Human Rights Watch, Innocence Project (USA), Instituto Nupef (Brazil), International

Commission on Missing Persons, Irish Council for Civil Liberties, KELIN (Kenya), Dylan Lim (Malaysia), Helena Machado (Portugal), Carole McCartney (UK); Yves Moreau (Belgium); Carly Nyst (UK/Australia); Pablo Palazzi (Argentina), Privacidade Brasil, Wafa Ben Hassine (Tunisia).Other consultees preferred to remain anonymous.

Work undertaken by GeneWatch UK in preparing and publishing this report was supported by a grant from the Foundation Open Society Institute in cooperation with the Information Program of the Open Society Foundations.

Contents

Introduction

The use of DNA evidence in criminal investigations has been a major advance in policing. When used wisely, DNA profiling can help to convict people who have committed serious crimes or exonerate people who are innocent. However, concerns arise when individuals' biological samples, computerised DNA profiles and personal data are collected indiscriminately or stored unnecessarily and/or indefinitely on a DNA database. There are concerns that this information could be used in ways that threaten people's individual privacy rights and those of their families. This highlights the importance of implementing safeguards regarding the collection, storage and use of biological samples and genetic data.

Throughout this document, we use the term "forensic databases" to refer to computer databases containing DNA profiles obtained from crime scene samples and/or from individuals for the purpose of investigating crimes. It is widely recognised that such databases raise important social and ethical issues that require widespread societal debate.[1]

Forensic DNA databases are now well established in many countries in the world. Rules governing what data can be collected and stored and how it can be used differ greatly between different countries. As DNA sequencing technology advances and becomes cheaper, there are plans to set up new databases or expand existing databases in many countries, sometimes driven partly by commercial interests.[2]

In some countries, databases that previously contained records only from people convicted of serious crimes are being expanded to include innocent people who have been arrested but not convicted and people convicted or given police warnings or other sanctions for minor crimes. These people are treated as belonging to a 'risky population' of people who are assumed to be likely to commit future offences.[3] In other countries, DNA databases of the whole population have sometimes been proposed.[4] Data-sharing, involving the transfer of information across international borders, is also on the increase (for example, via the EU's Prüm system, and via bilateral data sharing agreements between national governments and the United States).

Before policies are adopted to set up or significantly expand DNA databases, a detailed analysis of costs and a realistic appraisal of potential benefits are needed. Collecting and analysing large numbers of samples from persons who have no known connection to a crime is expensive, as is maintaining large databases. DNA databases that focus on collecting and storing crime scene evidence and DNA profiles from a more targeted population of known criminals, at high risk of reoffending, are more likely to be successfully implemented and to be cost-effective. Further, using DNA effectively during criminal investigations requires proper crime scene examination in a context of trained and reliable policing, a trusted chain of custody of samples, reliable analysis, and proper use of expert evidence in court.

Anyone who can access an individual's forensic DNA profile can use it to track that individual or their relatives. Access to a DNA sample, which can be further analysed, can potentially reveal more detailed information, for example about a person's health. Despite the seemingly authoritative nature of DNA evidence, it is not foolproof and mistakes can be made at crime scenes, in laboratories or in court.[5] However, there are currently no comprehensive international safeguards for forensic DNA databases that would protect people's privacy and other human rights, and prevent miscarriages of justice.

As countries develop legislation to govern DNA databases, it is important that civil society is engaged in the debate about what safeguards are needed to protect human rights. The International

Declaration on Human Genetic Data, which was adopted unanimously at UNESCO's 32nd General Conference on 16 October 2003, applies to the collection, processing, use and storage of human genetic data and biological samples, "*except in the investigation, detection and prosecution of criminal offences and in parentage testing that are subject to domestic law that is consistent with the international law of human rights*".[6] Therefore, more clarity is needed about what national legislation and international standards are required to protect such rights. Important principles enshrined in the United Nations Declaration on Human Rights include the right to privacy and a family life (Article 12), equality before the law (Article 7) and the right to the presumption of innocence and a fair trial (Article 11).[7] The United Nations Convention on the Rights of the Child is also relevant to children subject to forensic DNA analysis.[8]

This report is intended to facilitate the debate about human rights safeguards for forensic DNA databases by discussing the relevant issues and providing examples of best practice. More background information on how DNA databases operate is available in the GeneWatch UK briefing "DNA databases and human rights".[9]

Important questions include:

- Under what circumstances should the police be allowed to collect DNA and store samples and DNA profiles from individuals, from crime scenes, and from samples left behind elsewhere?
- Are there any procedures to destroy individuals' biological samples, DNA profiles or records when they are no longer needed?
- What age should people be before their DNA can be collected by the police and how should the rights of children and vulnerable persons be protected?
- What technical standards must be met by the DNA profiles before they are loaded to the database?
- Are quality assurance procedures being followed in the labs that analyse the DNA and at crime scenes, including for any analysis using portable machines outside the lab?
- What safeguards apply to the collection and analysis of DNA from crime scenes (including measures to prevent contamination, and rules for the use of commercial software to analyse mixtures of DNA from more complicated cases)?
- What rules should be put in place to prevent or limit access to DNA collected for non-criminal identification purposes (like DNA collected from family members to find missing persons, or DNA collected from soldiers)?
- What data is sent to whom and is it kept securely?
- Can the database and samples be used for additional purposes other than solving crimes?
- Is there any independent oversight and information about how the database operates?
- How are DNA matches used in court and is corroborating evidence needed?
- What information can be shared with investigators overseas?
- Are safeguards included in legislation, or only in guidelines that can easily be changed? Has there been sufficient public consultation?
- What rules should there be for police access to DNA collected for non-identification purposes (such as health, research, or ancestry testing)?

The Annexes include example text from existing laws around the world, to show how such issues have been addressed in practice, including some examples of how best practice might be implemented.

1. Whose data should be stored on a forensic DNA database?

In order to create a DNA database, biological samples (e.g. of blood or saliva) must be collected from individuals and crime scenes. DNA is extracted from these samples and analysed to produce a string of numbers, known as a forensic DNA profile, which can be stored on a computer database. This database can then be searched for matches between individuals' DNA profiles and crime scene DNA profiles. While a biological or DNA sample contains comprehensive genetic information about an individual, a forensic DNA profile contains only a limited amount of genetic information, which is however sufficient to establish the identity of an individual, family relationships, sex, and potentially some information about ancestry[10].

DNA evidence can be used in specific cases without building a DNA database. However, storing DNA profiles from unsolved crime scenes on a database allows a DNA profile from a new suspect to be searched against all past crime scene profiles to see if they are a suspect for any of these unsolved offences. The value of *entering* DNA profiles from individuals on a DNA database is that it may allow investigation of a past crime to be re-opened, by unexpectedly identifying a link between the suspect or a convicted criminal and a past crime. Two DNA profiles from different crimes may also match, allowing police to see that the same person may have committed both the crimes.

The purpose of *retaining* an individual's DNA profile on a database is to treat them as a suspect for any *future* crime. This is arguably likely to be of most benefit when an individual has a record as a "career criminal" and is considered likely to re-offend (*i.e.* retention of DNA profiles is justified by governments on the grounds that such DNA profiles may be useful to solve future crimes in the event of reoffending).[11] However, storing DNA profiles from named individuals raises important human rights concerns, because this information could be used for other purposes.

Important questions for legislators include:

- When should the collection of biological samples for DNA analysis be required or allowed?
- When should DNA profiles be entered on a database?
- When should biological samples be destroyed, and when should DNA profiles be removed from databases?

As well as considering the principles discussed below, policy makers considering establishing or expanding DNA databases will need to consider resources and priorities at the outset (see Section 9).

1.1. Collection of DNA

During the investigation of a crime, DNA may be collected from the crime scene and from individuals. These individuals may include persons suspected of committing the crime and volunteers, such as passers-by or victims, whose DNA is needed for elimination purposes.

Collection of DNA may be limited to convicted persons or may also include suspects. Suspects will include perpetrators of crimes but may of course also include innocent people. Many suspects are ultimately not convicted of an offence. Some of these suspects are never even arrested: those who are, are known as "arrestees". Some arrestees are never charged with an offence, or charges are dropped before a case gets to court. Other arrestees will be convicted or acquitted in a court of law. In some cases, a conviction will be overturned on appeal, or quashed many years later. In some countries, police may issue some penalties for minor offences without the case going to court (*e.g.*

police warnings, cautions and on-the-spot fines). It is important to consider all these categories of persons before deciding whose DNA may be collected and in what circumstances their DNA profiles may be retained on a computer database.

In addition, DNA samples are sometimes collected from large numbers of people in "mass screenings". Mass screenings are rarely successful unless the target group is small and narrowly defined, and have often been criticised for being used coercively, particularly against minority ethnic groups.[12] When used in this way, mass screenings are sometimes referred to critically as "DNA dragnets". Blanket and indiscriminate use of mass screenings implies a shift in the burden of proof in criminal procedures and can undermine the presumption of innocence.

UN Resolution 45/95 (Guidelines for the Regulation of Computerized Personal Data Files) states[13]:
"*1. Principle of lawfulness and fairness*
Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations".

An important over-arching issue is who is empowered to collect DNA from individuals and from crime scenes. It is important that the forensic specialists collecting evidence from crime scenes or analysing and interpreting DNA operate independently from the police, especially in countries where there is low public trust in the police, perhaps due to past miscarriages of justice or examples of corruption.

All countries which currently operate DNA databases have different rules for the collection of DNA with consent from volunteers and the collection of DNA without consent from some suspects and convicted persons.

1.1.1. Collection of DNA with consent from volunteers

The OECD's privacy protection principles include[14]:
"*1. Collection Limitation Principle*
There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

When DNA is collected from volunteers, it is established practice to seek fully informed consent from the individual. Fully informed consent is usually a requirement of privacy or data protection laws, but should also be written explicitly into DNA database legislation. To be valid, fully informed consent should be given for one or more specific purposes: it is not an open-ended agreement to any future use of a person's DNA.

The terminology "informed consent" first appeared in the World Medical Association's Declaration of Helsinki in 1964, which represents a pillar of the ethical principles in research ethics.[15] According to the definition given in the declaration the consent is only valid if it is properly informed and freely given (free of coercion, threats or persuasion). To be informed, consent should not be a mere yes or no answer. It is, indeed, a process in which those seeking the consent of the volunteers should clarify and specify the purposes of the collection and how the data will be used, etc. Detailed information must be provided, as described in Section 2.2, below. Other international instruments that outline

the importance of consent include the Universal Declaration on the Human Genome and Human Rights[16] and the Universal Declaration on Bioethics and Human Rights.[17]

Mass screenings are sometimes referred to as "DNA dragnets", when they are used inappropriately. In their book on DNA databases, Krimsky and Simoncelli argue: "*Written informed-consent procedures and proper protections against coercion should be in place for warrantless searches of non-suspect DNA samples when police engage in voluntary dragnets*", and "*DNA dragnets should be used by police only as a last resort and should be limited in scope to those who had access to the victim or who match a detailed description of the perpetrator. Those approached to provide DNA samples should be informed of their rights of refusal. Samples and profiles should be destroyed upon close of the investigation*". [18]

The EU Data Protection Directive 2016/680 [19] lays down the rules relating to the protection of individuals with regard to the processing of personal data (including genetic data) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences. It states in Recital (31): "*a clear distinction should, where applicable and as far as possible, be made between personal data of different categories of data subjects such as suspects, persons convicted of a criminal offence, victims and third parties, such as witnesses, persons possessing relevant information or contacts and associates of suspects and convicted criminals*".

A further safeguard for volunteers is to collect DNA only for a specific investigation, allowing the DNA profile to be compared with evidence from that crime scene only, without entering any information on a database.

Best practice includes written consent procedures for volunteers, which limit the use of their DNA profile to the specific investigation for which it has been collected, and which require the destruction of the biological sample as soon as practicable and expungement of the DNA profile at the end of the investigation, or as soon as the individual has been eliminated from the inquiry.

In the UK, the National DNA Database Ethics Group recommended in 2008 that volunteers' DNA profiles should not be loaded on to the DNA database and that all information and material should be destroyed after they are used. The Ethics Group found: "*Importantly, the work presented to the DNA Strategy Board illustrated that DNA matches between volunteer profiles and crime stains are satisfactorily achievable irrespective of whether or not the volunteer profiles are loaded from the analysing laboratory to the NDNAD* [National DNA Database]. *With the exception of sex offenders (who are sometimes sampled under the volunteer procedure), on the results to date, all of the matches useful to the police would have been obtained without speculative searching of the NDNAD. There would therefore be no loss to operational policing if, for the majority of crimes, volunteer samples were not loaded onto the NDNAD and were used only in relation to the investigation of the crime for which they were obtained*."[20] As a result, in the UK: "*It has decided that in future, volunteers who consent to provide a DNA sample for elimination purposes should no longer be asked to provide consent for their profile to be loaded to the NDNAD and these profiles will not be loaded*".[21]

The advantages of this approach are that it does not pose unnecessary risks to the privacy of volunteers, or expose them to potential miscarriages of justice if their profile is wrongly matched with a crime scene DNA profile in the future. Thus it helps to maintain public trust in police use of DNA and encourages people to agree to help the police with their investigations when it is directly relevant for them to provide their DNA.

Thus, best practices identified for the collection of volunteers' DNA include fully informed written consent for use in the specific investigation only, under the following conditions:

- No data is added to the DNA database;
- Samples are destroyed when the DNA profile is obtained (with, for example, a six month temporary storage period for quality assurance, see Section 1.2.1);
- DNA profiles are deleted automatically when the individual is eliminated from the inquiry (unless they are arrested and proceeded against, when the rules for arrestees apply, see Section 1.2.2);
- An easy-to-use mechanism must be available for people to check if they have been (unlawfully) added to the DNA database and an easy-to-use appeals process to an independent body must be available to get the profile removed if this happens;
- Retained data must not be used unlawfully to undertake additional searches and such matches should be inadmissible in court if they do occur.

Some examples of consent requirements in existing DNA laws are given in Annex A.

1.1.2. Collection of DNA without consent from suspects and convicted persons

It is widely recognised that it is acceptable to collect DNA without an individual's consent in some specific circumstances, which should be defined in legislation. Taking DNA from an individual without their consent, and storing their DNA profile on a DNA database, are interferences with their privacy, which can only be justified if necessary and proportionate to the need to tackle crime.

The Universal Declaration on the Human Genome and Human Rights, adopted unanimously at UNESCO's 29th General Conference on 11 November 1997, states:[22]
"*Article 9*
In order to protect human rights and fundamental freedoms, limitations to the principles of consent and confidentiality may only be prescribed by law, for compelling reasons within the bounds of public international law and the international law of human rights".

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*The taking of samples for the purpose of DNA analysis should only be carried out in circumstances determined by the domestic law; it being understood that in some states this may necessitate specific authorisation from a judicial authority.*
Where the domestic law admits that samples may be taken without the consent of the suspect, such sampling should only be carried out if the circumstances of the case warrant such action".[23]

Under US law, the taking of DNA samples falls within activities to which the Fourth Amendment, prohibiting unreasonable search and seizures, relates. Krimsky and Simoncelli argue that, for the purposes of the Fourth Amendment, "*[t]he taking of DNA constitutes a search. Therefore in order for the police to forcibly collect DNA from an individual suspected of a crime, they must have a warrant supported by probable cause*".[24] However, the Supreme Court case *Maryland v King* held that no warrant is required to collect DNA from suspects who have been arrested (arrestees) for serious crimes[25] and more than half of US states do now collect DNA from arrestees, although this practice remains contentious and safeguards vary greatly from state to state. For example, the Vermont Supreme Court has more recently held that the Vermont Constitution prohibits taking DNA from arrestees without a warrant.[26]

The collection of DNA from a suspect during an investigation can be justified when they are a suspect for a crime for which DNA evidence is directly relevant. Since the perpetrator of a crime may not wish to be identified, this provides justification for the collection of their biological sample, and

its analysis to produce a forensic DNA profile, without their consent. Legislation normally requires some form of prior authorisation of the decision to take the sample (for example, an order by a court based on evidence of "probable cause" that the suspect was involved in the offence), and restricts the circumstances in which DNA may be collected from individuals without their consent by limiting this process to more serious crimes for which the DNA evidence being collected is directly relevant. Some examples from existing DNA legislation are given in Annex B. Nevertheless, it should be noted that in some countries, such as Brazil, the constitutional right to silence can be interpreted as a right not to incriminate oneself, and this leads some to regard the collection of DNA for forensic purposes as unconstitutional (this issue is being considered by the Supreme Court in Brazil).

However, in some other countries, such as the UK, DNA is taken on arrest by the police for a very wide range of offences, without any independent authorisation. Since, in most cases, DNA is not relevant to the specific crime under investigation, the purpose of collection is usually to enter the individual's DNA profile on the DNA database, rather than to solve the specific crime of which they are accused.

Many countries restrict their DNA databases to contain the DNA profiles of convicted persons only, usually prisoners. However, other countries allow DNA profiles from suspects to be entered on the DNA database prior to conviction, and in some cases these DNA profiles are retained even if the individual is not convicted. Routine collection on arrest, with no independent oversight, risks police officers arresting people simply in order to obtain their DNA.[27] Alternatively, some counties in the USA (such as Orange County in Southern California[28]) allow charges to be dropped, or in some cases not even filed, in exchange for the provision a DNA sample. This is of particular concern if there are no provisions for the destruction of samples and the automatic removal of DNA profiles from the database if the individual is not charged or convicted (see Section 1.2). If the types of offences for which samples may be collected is not restricted, many people may be forced to give their DNA in circumstances where this is not justifiable by reference to any benefit in solving crimes.[29,30,31,32,33,34,35,36]This may include large numbers of children, in countries where DNA can lawfully be taken from them.

Large databases, created by collecting DNA routinely on arrest, are also more costly to manage and set up, and likely to be more prone to errors (see Sections 3 and 9).

There is no international consensus on when DNA can be collected from suspects and convicted persons, but important safeguards include:

- Restricting the categories of crimes for which DNA can be taken to more serious crimes, specified in legislation, for which DNA evidence is likely to be relevant;
- Requiring evidence of "probable cause" that the suspect committed the crime and some independent oversight of this, for example a decision by a court;
- Requiring automatic removal of the records of suspects who are acquitted or not charged from the DNA database, so that innocent people's records do not continue to be stored (discussed further in Section 1.2.2).

Defining the relevant categories of crimes requires public consultation and debate, taking account of the need to balance crime detection and prevention with protection of individual privacy and other rights (see Section 7) as well as issues of cost-effectiveness and optimal use of police resources (see Section 9).

1.2. Destruction of DNA and linked data

When DNA is taken from persons suspected of offences, some of these people will be innocent and will never be charged with or convicted of a crime. They may be acquitted by a court or the case may never come to trial. Even if convicted, they may have their conviction overturned on appeal. If innocent people's DNA profiles are retained against their will, this is a breach of their human rights.

Even if a person is convicted, they still retain some rights. For example, storage of a biological sample is not necessary to identify a person using DNA. Furthermore, storage threatens individual privacy as private genetic information can be revealed by analysing the sample. The storage of DNA profiles from convicted individuals may also become unnecessary over time, if there is no evidence that they are likely to commit further crimes for which their DNA profile might be relevant. Clear and specific guidance is therefore needed for decisions on whose DNA profiles ought to be retained.

The Grand Chamber of the European Court of Human Rights reached a unanimous judgment against the UK Government in 2008 for keeping innocent people's DNA profiles and samples, in contravention of Article 8 of the European Convention on Human Rights (the right to privacy).[37] The judgment in *S and Marper v United Kingdom* stated that "*the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society*". [38] The judgment applies in all 47 member states of the Council of Europe, covering 820 million citizens.

The UK Government has responded to the Marper judgement by removing innocent persons' records from its DNA and fingerprint databases and destroying all biological samples taken from individuals (whether convicted or not). The Protection of Freedoms Act 2012 led to the removal of over 1.7 million DNA profiles taken from innocent people and children from the UK DNA database and the destruction of 7,753,000 biological samples.[39] Specific provisions were applied to limit the retention of DNA profiles from children who had committed a single minor offence. Figures collected by the UK Government had shown that keeping innocent people's records on the DNA database did not help to solve more crimes and retaining samples raised privacy concerns whilst not being useful for identification purposes.[40] Following the significant reduction in the size of the DNA database the UK Home Office reported that "*The reduction in profiles held from innocent people has not led to any reduction in the number of matches the database produces*".[41]

When adopting new legislation since, most countries have sought to ensure that they are compliant with the Marper judgment, even if they are not members of the Council of Europe. An exception is found in some US States, which allow collection of DNA on arrest with no automatic expungement process. Brazil also lacks a specific regulation for the expungement of innocent people's records.

Krimsky and Simoncelli argue that: "*DNA data banks should be limited to DNA profiles from persons who are convicted of felonies*" and "*In cases where the DNA from a suspect is collected by way of a warrant, and the charges against that suspect are dropped or the individual is not convicted, the individual's DNA profile should be expunged automatically from the police record, and its biological source should be destroyed. Responsibility for expungement should rest with law enforcement: no petition or written request from the individual should be required*". [42]

1.2.1. Destruction of biological samples

Krimsky and Simoncelli argue that: "*Offender or suspect biological samples should be destroyed after DNA profiling so that the encoded information cannot be accessed for information beyond the DNA profile*".[43]

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*Samples or other body tissues taken from individuals for DNA analysis should not be kept after the rendering of the final decision in the case for which they were used, unless it is necessary for purposes directly linked to those for which they were collected*".[44]

Destruction of individuals' samples provides public reassurance that they will not be reanalysed to obtain additional sensitive information, such as information about health. In addition, this practice saves the costs of storage of large numbers of samples (which normally require refrigeration) and helps to prevent unauthorised access to genetic information. Destruction of samples may be regarded as an example of "privacy by design": an approach that promotes privacy and data protection compliance from the start of a project. It applies to samples collected from individuals, but not from crime scenes (see Section 1.2.7).

Sample destruction is widely practiced in many countries once the DNA profile, which is used for identification purposes, has been obtained. Temporary retention (usually a few months) is often allowed for quality assurance purposes (*i.e.* to allow random checks by analysing the stored sample and ensuring the second DNA profile that is obtained matches the first one). Examples of relevant legislative provisions are given in Annex C.

1.2.2. Provisions for the automatic deletion of innocent people's records

Retention of innocent people's DNA profiles undermines the principle of "innocent until proven guilty". Some suspects, who may have their DNA taken during an investigation, will be innocent and should not be treated as if they are convicted offenders.

Prior to the Marper judgement and the implementation of the Protection of Freedoms Act 2012, the retention of DNA profiles from innocent people in England and Wales was highly contentious.[45,46,47,48,49,50,51,52,53,54,55,56] Following the Marper ruling, most innocent people's DNA profiles are removed automatically from the UK National DNA Database, with provision for temporary retention in some cases (with oversight from the Biometrics Commissioner).
The rationale for retaining innocent people's DNA profiles – that this would solve more crimes – has been found to be incorrect.[57] Implementation of the Protection of Freedoms Act led to the deletion of over 1.7 million DNA profiles taken from innocent people and from children from the UK National DNA Database (NDNAD) and the destruction of all 7,753,000 DNA samples. The minister stated "*We have transformed the DNA database from one that infringed the privacy of over a million innocent citizens to one that is proportionate and still effective. In this we hope also to have transformed it from a contentious system that was seen as a threat to our liberties, to one that enjoys wide public support as an essential tool to fight crime*".[58] Despite earlier UK Home Office claims that the removal of records would reduce the value of the database, subsequent NDNAD annual reports have demonstrated continuing and increasing effectiveness.[59] Most countries have therefore accepted that it is best practice to have an automatic process for removal of DNA database records from persons who are not convicted. It is easier to incorporate the expungement process into legislation and practice before databases are set up or expanded than to apply such safeguards retrospectively. Thus an automatic expungement process may also be regarded as an example of "privacy by design". Privacy by design allows the process for the required expungements from all relevant (e.g. national and state) databases and backups to be built in at the start.

Examples of provisions for the expungement of innocent people's records from DNA databases are given in Annex D.

1.2.3. Review of data retention and limits on retention of DNA profiles from persons convicted of minor crimes

Many countries only collect DNA profiles from persons suspected or convicted of committing more serious crimes, such as rape and murder. However, some countries collect DNA when a person is arrested on suspicion of committing relatively minor crimes, even where DNA evidence plays no role in the investigation, and retain DNA profiles indefinitely on conviction. In the UK, police cautions (warnings issued by the police on admission of a person's guilt, without the need for a trial) also count as convictions and lead to the retention of a person's DNA profile until after death (the deletion date is set at age 100), unless the person was a child at the time of the offence. However, automatic deletion after fixed time frames, or at least review of the need for retention, is required for children in the UK and for adults in some other countries (see examples in Annex E).

UN Resolution 45/95 (Guidelines for the Regulation of Computerized Personal Data Files) states in Article 3(c) that it should be ensured that[60]:
"*The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified*".

The EU Data Protection Directive 2016/680 [61] states (28): "*The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review*". Article 5 provides for time limits of storage and review, stating: "*Member States shall provide that appropriate time limits are established for the erasure of personal data or for a periodic review of the need for the storage of the data. Procedural measures shall ensure that these time limits are observed*". Article 16 (2) states that: "*Member States shall require the controller to erase personal data without undue delay and provide for the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where processing infringes the provisions adopted pursuant to Article 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject*".

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*Measures should be taken to ensure that the results of DNA analysis and the information so derived is deleted when it is no longer necessary to keep it for the purposes for which it was used. The results of DNA analysis and the information so derived may, however, be retained where the individual concerned has been convicted of serious offences against the life, integrity or security of persons. In such cases strict storage periods should be defined by domestic law*".[62]

Thus, best practice requires legislation to review the need for retention of DNA profiles and to limit the timeframes for retention, particularly in less serious cases and/or if the offence was committed by a child. Examples of provisions in existing legislation are given in Annex E.

1.2.4. Appeals process against retention of data

Many countries allow individuals to find out what personal data is held about them and to appeal against retention of their data. Best practice should include an independent and transparent process for individuals to request removal of their records, in addition to an automatic process to remove innocent people's records.

The OECD's privacy protection principles include[63]:
"***7. Individual Participation Principle***
An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him
i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner; and
iv) in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."

The EU Data Protection Directive 2016/680 [64] states (40): "*Modalities should be provided for facilitating the data subject's exercise of his or her rights under the provisions adopted pursuant to this Directive, including mechanisms to request, free of charge, access to his or her personal data, as well as rectification, erasure and restriction. The controller should be obliged to respond to requests of the data subject without undue delay, unless the controller applies limitations to data subject rights in accordance with the rules of this Directive…*".

In Brazil, the *habeas data* law provides similar, but more limited, protections.[65] *Habeas data* (in different forms) applies in a number of other Latin American countries (*e.g.* Colombia, Paraguay, Peru, Argentina, Costa Rica). *Habeas data* can be sought by any citizen against any manual or automated data register to find out what information is held about his or her person. In Brazil, the Constitution only allows for the access to and the correction of data, not for its update or destruction. Compared to EU Data Protection, Latin American *Habeas data* fulfils at least requirements of transparency, rectification, update (in some countries), accuracy and purpose, but that not all versions of Habeas Data provide security provisions, and none place restrictions on transfer to other countries (discussed further in Section 6).[66]

Some examples of relevant provisions are given in Annex F.

1.2.5. Deletion of linked data on other databases

The same principles of data protection described above require that linked data on other databases (*e.g.* police record of arrest, fingerprints) should be deleted at the same time as DNA database records.

A retained record of arrest can lead to the refusal of a job[67] or visa[68] or to harassment by the police. Further, assumptions about the likelihood of offending, which may be made based on this retained data, can exacerbate racial bias (see Section 2.3).

In 1997 a Bulgarian national was entered in the police registers in his country, with reference to a rape, as an "offender", after being questioned about a rape, even though he had never been indicted for the offence. He was later subjected by the police to a number of checks related to rape complaints or disappearances of young girls. The European Court of Human Rights found that this was a violation of Articles 8 (right to respect for private and family life) and 13 (right to an effective remedy) of the European Convention on Human Rights.[69]

1.2.6. Exceptions for national security

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*Where the security of the state is involved, the domestic law of the member state may permit retention of the samples, the results of DNA analysis and the information so derived even though the individual concerned has not been charged or convicted of an offence. In such cases strict storage periods should be defined by domestic law*".[70]

Exceptions for national security are likely to be contentious. They should be openly debated and defined in law.

For example, in the UK, the Protection of Freedoms Act allows DNA profiles to be retained on the National DNA Database following a "national security determination", issued in writing by the responsible chief officer of police, if the officer determines that retention is necessary for the purposes of national security.[71] National security determinations last two years, but may be renewed. They are subject to review by the independent Biometrics Commissioner, who may order destruction of the data if he determines that retention is unnecessary.[72] The Commissioner publishes an annual report.[73]

1.2.7. Retention of crime scene evidence

Notwithstanding the need for limits on the retention of individuals' data, described above, best practice includes retaining crime scene DNA evidence in case a re-investigation is needed or becomes possible as a result of new technology. Biological samples collected from crime scenes might require reanalysis at a future date if the perpetrator is not identified immediately or if there is concern about a possible miscarriage of justice in the case.

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*Samples and other body tissues, or the information derived from them, may be stored for longer periods:*
- when the person concerned so requests; or
- when the sample cannot be attributed to an individual, for example when it is found at the scene of an offence".[74]

2. Safeguards for the process of collecting DNA

2.1. Collection of biological samples

Many countries make a distinction between "intimate" and "non-intimate" samples. Intimate samples can usually only be taken by medical professionals, with consent (*e.g.* samples of blood, semen or vaginal swabs). Non-intimate samples (mouth swabs or hairs other than pubic hair) can sometimes be taken without consent from offenders and/or suspects (see above) and non-intimate sampling can often be undertaken by other technical staff, including trained police officers. Intimate samples should never be taken without consent and normally are taken only in specific cases where such samples provide important evidence, such as from the victim of a rape.

Taking a (non-intimate) sample without consent may require the use of "reasonable force" (for example, pulling hairs from someone's head) if the person involved refuses to open their mouth to allow the taking of a swab.

Legislation should define who has the power to collect samples, for what purposes and specify appropriate, secure locations (such as when a person is held in detention) and training. Some examples of legislative provisions for DNA sampling are given in Annex G. Particular attention must be paid to the needs of vulnerable persons, such as children, ethnic minorities and people who are disabled or mentally ill (see Annex H). Children should not be treated as suspects unless they have reached the age of criminal responsibility. However, for children who have done so, special provisions will be needed regarding: (1) when they are deemed competent to give informed consent to the collection of DNA samples; (2) when samples may be collected without consent; (3) the provision of relevant information; and (4) the presence of a responsible adult during the collection process. Similar issues apply to persons who are deemed to be incapable of giving fully informed consent for reasons other than age, such as mental illness or intellectual disability.

2.2. Provision of information for all persons from whom DNA is taken

UN Resolution 45/95 (Guidelines for the Regulation of Computerized Personal Data Files) states[75]:
"*4. **Principle of interested-person access***
Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence".

The OECD's privacy protection principles include[76]:
"*7. Individual Participation Principle*
An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him
i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner; and
iv) in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."

Best practice involves including a requirement in legislation to provide information to individuals (whether volunteers or suspects) on why their sample is being taken and what their rights are, so that they may exercise these rights, for example by allowing people to object if their privacy is breached or their data is not expunged when necessary. Examples are given in Annex I.

Information provision is needed for persons whose DNA is taken with and without consent. However, in order to fulfil the requirement for fully informed consent from volunteers, a written informed consent form is necessary but not sufficient; in fact, it is important to verbally clarify the

purposes for obtaining the data, and ensure that such explanation is tailored for the specific individual and their abilities to understand it. The information given verbally and in writing on the consent form to be signed should be as comprehensive as possible, stating the purposes, the risks, uses of the data and the possible consequences, how long the sample and data will be retained, and how to check whether information or material is unlawfully retained and how to appeal against this. This helps to guarantee respect for individuals and their rights as well as public trust.

2.3. Minimising the potential for racial bias

DNA databases have often been controversial because of racial bias with respect to the selection of those individuals who are subject to DNA testing and retention.[77,78]

This bias results from multiple causes throughout the criminal justice systems in the UK and the USA. There is no single legislative provision that can eliminate racial bias with regard to whose records are kept on a DNA database. However, it is clear that the retention of DNA profiles from innocent persons who have been arrested but not convicted of offences will exacerbate such bias.

UN Resolution 45/95 (Guidelines for the Regulation of Computerized Personal Data Files) states[79]:
"*5. **Principle of non-discrimination***
Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.
*6. **Power to make exceptions***
Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.
Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles I and 4, may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination".

The EU Data Protection Directive 2016/680 [80] states in Article 11(3): "*Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law*". These categories are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Best practice will involve a combination of legal provisions preventing discrimination, combined with in-depth consideration of the effect of policies on ethnic minorities.

3. Safeguards for the analysis of DNA

3.1. Collection of DNA from crime scenes and protection of the chain of custody

Best practice legislation requires a clear definition of crime scene evidence, so that police are not allowed to collect DNA that people have left behind elsewhere (for example, on a coffee cup in a shop or at a political meeting), unless the location is part of a criminal investigation.

Crime scenes should be promptly examined if DNA evidence is likely to be relevant, and quality assurance procedures must protect against contamination of evidence and protect the chain of custody of the evidence from the crime scene to the laboratory to the court. Crime scene treatment, to a large extent, predetermines the quality and quantity of information available for intelligence processes, investigation and ultimately for court evidence.[81]

The benefits of a DNA database are driven largely by the number of *crime scene* DNA profiles collected, not by the number of individuals' DNA profiles.[82] In the USA, the Urban Institute found that for every 1,000 offender profiles uploaded to the DNA database, 8 investigations were aided, whereas for every 1,000 crime scene DNA profiles uploaded, 407 investigations were aided[83]. Thus, it is important to prioritise the collection of DNA profiles from crime scenes, rather than from individuals. Prompt analysis may allow offenders to be caught and convicted, potentially preventing further serious crimes. Failure to analyse DNA collected from rapes has led to significant controversy in many US states, and new laws have been proposed in many states to mandate testing of DNA rape kits within a fixed timeframe.[84,85,86] Some example legal provisions on prompt crime scene examination are given in Appendix J.

Although laboratories also need quality assurance (see Section 3.2), a major cause of misidentification using DNA is mix-ups or contamination of samples before they reach the lab.[87] A person's DNA can also be transferred to a murder victim or a weapon, even if they never touched it.[88] For this reason, only trained crime scene examiners should collect DNA evidence from crime scenes and quality assurance procedures and inspections are needed to minimise the risk of mix-ups and contamination, which might otherwise lead to miscarriages of justice.[89] Properly securing crime scenes is also critical.[90]

In the UK, the Forensic Science Regulator has issued draft guidance on the control and avoidance of contamination in crime scene examination.[91] In the USA, the Technical Working Group on Biological Evidence Preservation has produced a relevant report.[92] However, not all countries yet have the relevant technical experts to develop and implement best practice. For example, the police in many developing countries such as India and Trinidad and Tobago are poorly resourced and may fail to secure crime scenes.[93,94]

Best practice requires regulation of the whole chain of custody, not just laboratories. The UK has a Forensic Science Regulator which monitors compliance, investigates errors and prepares guidance on issues such as the avoidance of contamination.[95] Some US states have similar arrangements, such as the New York Office of Forensic Services.[96]

3.2. Laboratory quality assurance

There is widespread agreement that forensic laboratories should implement international standards of quality assurance, to avoid the mix up, contamination, or misinterpretation of evidence leading to

miscarriages of justice. Analysis of DNA for forensic purposes should take place only in laboratories with quality assurance.

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*DNA analysis is a sophisticated scientific procedure which should only be performed by laboratories possessing the appropriate facilities and experience.*
The member states should ensure that a list be drawn up of accredited laboratories or institutions which satisfy the following criteria:
- high professional knowledge and skill, coupled with appropriate quality control procedures;
- scientific integrity;
- adequate security of the installations and of the substances under investigation;
- adequate safeguards to ensure absolute confidentiality in respect of the identification of the person to whom the result of the DNA analysis relates; and
- guarantees that the conditions laid down by this recommendation are followed.
The member states should institute a means of exercising regular supervision of their accredited laboratories".[97]

The most frequent source of errors is mix-ups or contamination of samples, either at the laboratory or before the samples get there.[98] Errors are also more likely to occur where DNA from a crime scene contains a mixture of cells from more than one person (which is often the case in rape cases).[99,100,101] People who have been affected by mix ups of DNA samples include a teenager in England who spent three months behind bars for rape in a city he had never even visited;[102] and an 18 year old in Las Vegas who spent 4 years in jail for a robbery committed by his cousin.[103] In Houston, Texas, DNA samples were tampered with or contaminated and one result was that teenager Josiah Sutton was convicted and sentenced to 25 years in prison for a rape he did not commit.[104] In New York, a student protestor was wrongly linked to a killing by DNA collected while she was protesting.[105] In England, Peter Hamkin was held by police for 20 days for an alleged murder in Italy, before it was discovered that a mistake with the DNA evidence had been made by Interpol.[106]

Recent developments in technology mean that crime scene DNA may be analysed in mobile laboratories or using portable equipment. Best practice would require such methods to be subject to the same quality standards as analysis in a laboratory. In addition, the existence of portable DNA analysis should not be allowed to undermine the safeguards required for the collection of DNA from individuals (outlined above).

Example legal provisions on laboratory quality assurance – requiring independent accreditation and audits - are given in Appendix K.

3.3. Provision, status and oversight of forensic laboratories

Forensic DNA laboratories may be run by the state or privately. In addition to being regulated so that quality assurance procedures are in place (Section 3.2), sufficient provision needs to be in place to prevent backlogs, particularly in crime scene DNA analysis.

Laboratories where there is insufficient training or which lack resources can lead to delays or miscarriages of justice.[107,108,109]

Public confidence is likely to be increased if forensic laboratories are independent of the police and if the methods used are open and transparent and overseen by independent regulators. A government-owned but arms-length body, with an independent regulator, may be the best approach. In the UK, the national Forensic Science Service (FSS) was originally part of the

Government Home Office, but became an executive agency of the Home Office in 1991 and a trading fund in 1999, enabling increased independence from the Government. However, in 2005, it became a government-owned company, with a view to privatisation of all forensic services. In 2008 a Forensic Regulator was set up, amid increasing concern about forensic standards as more commercial competitors came onto the market. In 2012, the FSS was shut down by the Government, due to losing money, and DNA testing was being conducted by a combination of commercial and police laboratories. By 2016 there were reports that a new national forensic science service was planned, amid concerns about poor value for money of commercial services, and problems with quality and gaps in services.[110]

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*While acknowledging that the intellectual property rights associated with particular methods of DNA analysis may be vested in certain laboratories, member states should ensure that this does not impede access to the use of DNA analysis*".[111]

3.4. DNA profiling standards

DNA profiling standards must be sufficient to minimise false matches occurring by chance. This must take account of increased likelihood of false matches in transboundary searches, and with relatives.

A DNA profile consists of a string of numbers based on parts of the chemical DNA which is found in every cell in a person's body (for example, their blood or saliva). The DNA profile consists of pairs of numbers based on the number of repeats of a short sequence of DNA found at several particular locations in the strong string of chemical letters that makes up an individual's DNA. For example, a ten loci DNA profile uses ten locations along the DNA, usually on different chromosomes, a twelve loci DNA profile uses twelve: the more loci that are used the less likely it is that two DNA profiles from different people will be the same. DNA profiles also use a genetic marker which identifies whether the person is male or female.

The likelihood of errors increases the larger the database is, because more samples are being analysed and more computer searches are being conducted. The expected number of false matches that will occur by chance ("adventitious matches"), assuming there are no errors or mix-ups at the crime scene or the lab, is given by the probability of a false match (*i.e.* a match with a DNA profile from the wrong person) times the total number of comparisons made between DNA profiles.

As more searches are done, it has become necessary to increase the number of loci used in DNA profiles stored on DNA databases in the US and European countries to minimise the number of adventitious matches. However, storing individuals' samples to allow for re-analysis is expensive and poses unnecessary risks to privacy (see Section 1.2.1). Therefore, an important element of best practice is for a country to choose a profiling system that is likely to be adequate before it starts to build a database. The profiling system should minimise the expected number of adventitious matches, taking account of the number of searches that are likely to be made, both within that country and with foreign databases. The probability that two brother's DNA profiles match by chance is much higher than for two unrelated individuals, because family members share parts of their DNA.[112,113] It may be particularly important to account for this, by increasing the number of loci in the profiling system used, in countries where the average family size is large.

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*The member states should promote standardisation of the methods of DNA analysis both at national and international levels. This may involve inter-laboratory collaboration in validation of the analytical and control procedures*".[114]

Particular problems arise with analysing very small samples of DNA, or with mixtures of more than one person's DNA. In some cases, commercial computer software has been used to try to identify an individual's DNA profile from a mixture: however such results are always open to interpretation.[115,116] It is important that any algorithms can be independently validated and that their limitations are known to the police and to the courts. Disputes over interpretation also highlight the need for corroborating evidence to be required in court (Section 5.1).

Example legal provisions on DNA profiling standards are included in Annex L.

3.5. Elimination databases for police or other staff who might contaminate samples

Whilst volunteers are members of the public (often victims of a crime) whose DNA profiles are needed for elimination purposes for a specific offence (see Section 1.1.1), there is a different category of persons, *i.e.* police, laboratory and medical workers, whose DNA profiles should be stored on a database if their work might lead to contamination of crime scene samples, either during the process of examination of a crime scene (where a police officer might leave their DNA) or during the laboratory analysis of samples. Strictly speaking these persons are not volunteers, as providing a sample may be a condition of their work. Databases of their DNA profiles are usually kept on separate elimination databases, as these persons are neither suspects nor convicted persons: in the case of medical and laboratory staff these databases may be managed by the hospital or laboratory where they work, rather than being shared with the central or state government. Provisions should be also made for deletion of staff DNA profiles when retention is no longer necessary.

The UK's Forensic Science Regulator has published a detailed report on the importance of elimination databases.[117] The costs of establishing one or more Laboratory Elimination Database(s) (LEDs), Police Elimination Database(s) (PEDs) and Medical Examiners Elimination Database(s) (MedExDs) should be included in the costs of implementing DNA database legislation. Best practice involves maintaining these databases separately from the criminal DNA database and restricting searches to those that are necessary to identify contamination.

Annex M contains examples of legislative provisions for elimination databases.

4. Safeguards for the storage and uses of DNA and linked data

4.1. Stored forensic DNA profiles should be restricted to non-coding DNA

A person's DNA contains private information about (1) physical characteristics of the individual and (2) some health conditions, such as genetic disorders, and the risk of the individual passing these conditions on to his or her children. Currently, sex is an important physical characteristic that is systematically assessed as part of forensic DNA profiling because of its relevance to criminal investigations and as a quality control. Other than a person's sex, private information about an individual's physical characteristics or health risks is irrelevant to matching their DNA profile with DNA profiles obtained from criminal investigations and is not needed for identification purposes. Although the role of DNA in disease is complex, forensic DNA profiles generally focus on individual differences in "non-coding" DNA (the parts of the DNA that do not code for proteins that play important biological functions in the human body). Although such markers can sometimes be

statistically associated with disease within a family, they are not predictive of disease in the general population.[118] Legislation should therefore specify that only forensic DNA profiles are extracted and stored in DNA databases and that they are based on non-coding DNA that provides no information on a person's health risks or physical characteristics (other than their sex).

Example legal provisions are given in Annex N. It is important that the forensic DNA profile is correctly defined in legislation (as non-coding DNA) and that the legislation also establishes that biological samples collected from individuals (which include the coding parts of DNA) are discarded promptly (see Section 1.2.1) and that they will not be used for other purposes.

An exception to the use of forensic DNA profiles based solely on non-coding DNA in criminal investigations has sometimes occurred where a crime scene DNA profile does not match any stored DNA profile and no suspect has been identified. In such cases, the crime scene sample has sometimes been further analysed to extract additional genetic information, in order to seek to predict some identifying characteristics of the suspect, such as their hair or eye colour, or their ethnicity (ancestry), or even to try to produce a computer-generated picture of what their face might look like.[119] This emerging application of DNA analysis is known as "phenotypic profiling" or "DNA phenotyping" (a person's "phenotype" is all the observable characteristics of that individual) and is being sold as a commercial service to some police forces. However, phenotypic profiling is controversial because predictions made from genetic information are often poor and might mislead police investigations and/or lead to misdirected targeting of minority ethnic groups for their DNA.[120,121] Both these problems occurred in the past in a police investigation of a series of rapes in London (known as Operation Minstead), during which police wrongly predicted which Caribbean Island the suspect came from, based on his DNA.[122] Therefore, if phenotypic profiling is to be used at all in police investigations in the future, it will require strict regulation. Importantly, even if this technique were more successful, it does not require DNA databases to contain any information other than forensic DNA profiles. This is because phenotypic profiling would only ever be of use in specific cases, to test unmatched crime scene DNA, and is never needed when searching for matches with DNA profiles stored on a database.

Another new challenge is the potential introduction of Next Generation Sequencing (NGS). NGS is a term used to describe DNA sequencing technologies whereby multiple pieces of DNA are sequenced in parallel. This allows large sections of the human genome to be sequenced rapidly. These technologies provide more wide-ranging information than standard forensic DNA profiling. Declining costs increase the feasibility of the introduction of NGS for forensic DNA databases, however, many important ethical issues arise.[123] Potential benefits could arise from more detailed sequencing in some circumstances (for example, for degraded DNA from crime scenes or mass disasters). However, there is no reason to risk revealing private information by allowing the sequencing of coding DNA for profiles stored in criminal DNA databases.

4.2. Separation of criminal and non-criminal databases (e.g. missing persons' databases)

Legislation on forensic DNA databases often includes a role for DNA databases in identifying missing persons or body parts. Normally, this process requires DNA from relatives, so that the unknown DNA profile can be compared to look for a partial match. In other cases, DNA may be available from the person who has been reported missing (for example, from their toothbrush). However, care must be taken to ensure that missing persons and their relatives have their rights protected: they are not criminals or suspects.

A definition of a "missing person" should be included in legislation. Without a definition, the state could use the missing person's database or index to track persons of interest (such as political opponents) in circumstances where a person has moved to an unknown location but there are no concerns for their safety or well-being.

In addition, best practice includes storing DNA profiles from missing persons and their relatives in databases that are kept separately from criminal DNA databases and restricting searches to finding the missing person, not seeking to identify matches with DNA profiles from crime scenes. An important advantage of keeping these databases separate from other DNA databases is to reassure relatives of missing persons that the use of their stored profiles will be restricted to searching for their missing relative. Fully informed consent should be required from relatives as such searches are a voluntary process. An exception can be made for unidentified bodies or body parts, where a search against a criminal DNA database may be useful for identification purposes. Provisions are also needed for the destruction of biological samples when they are no longer needed and deletion of profiles on request or at the end of an investigation.

The need to separate databases that serve non-criminal purposes also applies to other databases established with consent for identification purposes, such as DNA databases of people serving in the armed services, which may be used to identify them if they are missing in action.

Example legal provisions for missing persons' DNA databases are given in Annex O.

4.3. Requirements for independent and transparent governance

Governance of DNA databases varies widely in different countries.[124]

Best practice for DNA databases includes an independent and transparent system of governance, with regular information published (*e.g.* annual reports and minutes of oversight meetings). Multi-stakeholder governance is preferable, including civil society and experts on genetic privacy. There must be adequate public and regulatory scrutiny to ensure the database is compliant with the law and to maintain public confidence.

The OECD's privacy protection principles include[125]:
"***8. Accountability Principle***
A data controller should be accountable for complying with measures which give effect to the principles stated above."

The Nuffield Council on Bioethics states[126]:
"*In this chapter we emphasise the importance of robust ethics and governance oversight of forensic databases, both as a means to protect the liberty, autonomy and privacy of those whose details are recorded on such databases, and also to help engender public trust and confidence in their existence and use as part of a criminal justice system. The potential uses and abuses of forensic databases are considerable. Effective governance helps to ensure not only that their utility is maximised, but also that their potentially harmful effects – such as threatening privacy , undermining social cohesion and aggravating discriminatory practices – are minimised. Good governance can anticipate and respond to new challenges; it is not merely a means to impose sanctions once things go wrong. Moreover, open governance can address suspicion and promote support among the public for an enterprise which, after all, is essentially in the public interest*".

In the UK, the police were given powers to collect and store DNA long before a statutory system of governance was put in place by the Protections of Freedoms Act 2012. The Act followed major public

controversy about the database. Comparing the systems of governance in the UK and the Netherlands, one researcher concludes: "*If one cherishes civil rights, then the Dutch model of legislating forensic DNA databasing and its practices first, and only subsequently implementing those technologies is superior to that of the English model of using forensic genetics without formulating dedicated legislative provisions regarding the* [UK] NDNAD [National DNA Database]".[127] Oversight in the UK has improved since the Protection of Freedoms Act 2012. Governance is now undertaken by several bodies: the National DNA Database (NDNAD) Strategy Board[128], the NDNAD Ethics Board[129], the Biometrics Commissioner[130], the Forensic Regulator[131], and the Information Commissioners Office[132] (ICO), which ensures compliance with data protection law. Annual reports and minutes of meetings are publicly available. Other examples of committees with oversight of DNA databases include the Rede Integrada de Bancos de Perfis Genéticos (RIBPG) in Brazil[133] and the National Forensic Oversight and Ethics Board (NFOEB) in South Africa.

Public trust may also be enhanced if DNA databases are maintained independently from the police and government. Independence from the police is likely to be an important consideration for public support of forensic DNA databases in many countries. For example, legislation may require forensic laboratories to be run independently and the computer database to be maintained by an independent body. Legal mechanisms must exist to ensure citizens have access to due process, and to ensure adequate oversight and the ability to revise decisions.

Example provisions on governance of DNA databases are given in Annex P.

4.4. Access restrictions and accuracy and security of data

The Universal Declaration on the Human Genome and Human Rights states:[134]
"*Article 7*
Genetic data associated with an identifiable person and stored or processed for the purposes of research or any other purpose must be held confidential in the conditions set by law".

UN Resolution 45/95 (Guidelines for the Regulation of Computerized Personal Data Files) states:
"*2.* ***Principle of accuracy***
Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed".

And:
"*7.* ***Principle of security***
Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses".

Access to DNA databases and biological samples must be restricted and any transfer of data (*e.g.* from police station to lab or database) must be secure for a DNA database to be compliant with best practice. Shared data must be minimised so that data is shared only when necessary. For example, personal identification information should not be sent with samples to laboratories, and anonymisation and encryption should be used whenever sharing personal information is unnecessary.

Over 100 countries and independent jurisdictions and territories around the world have now adopted comprehensive data protection/privacy laws to protect personal data held by both governments and private companies.[135,136] There is a recognised core set of data protection principles which are[137]:

1. Openness:
Organizations must be open about their personal data practices.
2. Collection limitation
Collection of personal data must be limited, lawful and fair, usually with knowledge and/or consent.
3. Purpose specification
The purpose of collection and disclosure must be specified at the time of collection.
4. Use limitation
Use or disclosure must be limited to specific purposes or closely related purposes.
5. Security
Personal data must be subject to appropriate security safeguards.
6. Data quality
Personal data must be relevant, accurate and up-to-date.
7. Access and correction
Data subjects must have appropriate rights to access and correct their personal data.
8. Accountability
Data controllers must take responsibility for ensuring compliance with the data protection principles.

These eight principles appear in some form in all of the key international and regional agreements and guidelines regarding data protection. An additional principle - data minimization - only appears in the EU Data Protection Directive (and the new EU General Data Protection Regulation), but has considerable global influence[138].

In the EU and many (but not all) other countries, DNA databases are covered by data protection and/or privacy laws. For example, the EU Data Protection Directive 2016/680 specifies that personal data used for the investigation of criminal offences should be processed in a manner that ensures an appropriate level of security and confidentiality, including by preventing unauthorised access to or use of personal data.[139] Compliance is overseen by Data Protection Officers and supervisory authorities (Information Commissioners). There is a requirement for privacy by default and design, so that access to identifiable data is limited.

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*The collection of samples and the use of DNA analysis must be in conformity with the Council of Europe's standards of data protection as laid down in the Data Protection Convention and the recommendations on data protection, in particular Recommendation No. R (87) 15 regulating the use of personal data in the police sector*".[140] Recommendation No. R (87) includes data protection safeguards that have been widely adopted across Europe, although further safeguards have been recommended since.[141,142]

The OECD's privacy protection principles include[143]:
"*5. Security Safeguards Principle*
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."

Although the USA lacks comprehensive privacy legislation, there is a federal statute (42 U.S.C. § 14132[144]) that imposes privacy requirements on states that are part of the Combined DNA Index

System (CODIS), and US states that collect DNA also have laws that prohibit it from being used for improper purposes, although the details of these laws may vary.

However, China, which has a large DNA database, is among the countries that lack privacy legislation, and some countries which are planning or beginning to construct DNA databases, such as Brazil and India[145], have draft privacy laws that have yet to be finalised or adopted.

It is clear that access to databases and samples must be restricted by legislation to avoid misuse. In the absence of data protection or privacy laws, security of data may be regulated when it is held on a central database, but not necessarily as it is transferred between police stations, laboratories, the database and the courts.

Annex Q contains example provisions for the security of data.

4.5. Restrictions on uses of stored data

The OECD's privacy protection principles include[146]:
"*3. Purpose Specification Principle*
The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation Principle
Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
a) with the consent of the data subject; or
b) by the authority of law."

UN Resolution 45/95 (Guidelines for the Regulation of Computerized Personal Data Files) states[147]:
"*3.* ***Principle of the purpose-specification***
The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:
(a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified;
(b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;
(c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified".

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*Samples collected for DNA analysis and the information derived from such analysis for the purpose of the investigation and prosecution of criminal offences must not be used for other purposes*".[148] However, "*Samples taken for DNA analysis and the information so derived may be needed for research and statistical purposes. Such uses are acceptable provided the identity of the individual cannot be ascertained. Names or other identifying references must therefore be removed prior to their use for these purposes*".

The EU Data Protection Directive 2016/680 [149] states (26): "*In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the*

collection of the data" and (29) "*Personal data should be collected for specified, explicit and legitimate purposes…*".
Article 4 (1)b requires that personal data must be "*collected for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes*".

Council of Europe Recommendation No. R (97) 5 on the Protection of Medical Data states[150]:
"*4.8. Processing of genetic data for the purpose of a judicial procedure or a criminal investigation should be the subject of a specific law offering appropriate safeguards.*
The data should only be used to establish whether there is a genetic link in the framework of adducing evidence, to prevent a real danger or to suppress a specific criminal offence. In no case should they be used to determine other characteristics which may be linked genetically".

In general this means that uses of forensic DNA databases should be restricted by law to solving crimes or identifying dead bodies or body parts. Identification of a person is not necessarily an acceptable use, if the individual is not a suspect for a crime. Best practice for missing persons' databases (if they exist) is to keep them separate from police databases, as described in Section 4.2.

Research uses can be restricted to anonymised verification of database performance (*e.g.* checking false matches etc.) to prevent breaches of ethical requirements to conduct genetic research only with fully informed consent (as required, for example, by the Universal Declaration on the Human Genome and Human Rights[151] and the International Declaration on Human Genetic Data[152]). Third party access to anonymised data for such limited purposes (*i.e.* directly related to the specified purpose of collection of the data) may be allowed, and could enhance public trust in the database provided public information on research projects is published. Best practice includes an independent ethics board to oversee applications for research, as required by the relevant international declarations. Research uses for other purposes (*e.g.* health research, behavioural research) should not be allowed, if the database is to be compliant with international ethical standards.

Destruction of samples (see Section 1.2.1) is an important additional safeguard to prevent the analysis of additional genetic information, in particular in relation to potential health or behavioural traits.

Examples of provisions restricting the uses of forensic DNA databases are given in Annex R, and example provisions on research uses are provided in Annex S.

4.6. Restrictions on the use of familial searching

Familial searching is a process by which investigators look for partial matches between crime scene DNA profiles and the DNA profiles of individuals stored on a DNA database. This can be used to identify a relative of the suspect who can then be interviewed, potentially leading to the suspect's identification and perhaps a successful prosecution. Familial searching leads to a long list of partial matches which must be shortened by additional DNA testing and/or other police work. Familial searching has helped to solve a number of serious crimes. However, it raises additional concerns about the privacy of individuals who are not suspects but who may be related to a suspect.[153,154,155,156,157,158] In particular, instances of non-paternity might inadvertently be revealed through the process of familial searching. If used routinely, familial searching could lead to significant abuses by allowing investigators or anyone who infiltrates the database to track down the relatives of political dissenters, pursue enemies, or identify paternity and non-paternity for personal, commercial or criminal reasons. This is one reason why there should be strict legislative rules on whose DNA profiles can be stored on police databases (see Section 1). However, restrictions on when familial searching can be used are also needed, for example by restricting its use to serious,

unsolved crimes, when all other investigative routes have been exhausted. In Brazil, the constitutional principle of the individual nature of penalties could be interpreted as a barrier to familial search.

Krimsky and Simoncelli argue that: "*Police seeking to acquire and analyse the DNA of family members of an individual identified through a partial match must obtain a warrant*".[159]

Example provisions on the use of familial searching are at Annex T.

5. Safeguards for the use of DNA evidence in court

5.1. Use of DNA evidence in court

Expert evidence and statistics must not misrepresent the role and value of the DNA evidence in relation to the crime. Due account must be taken of how a person's DNA may have arrived at a crime scene, including the possibility of contamination. An important safeguard is to require prosecutions to submit corroborating evidence so that they are not based on a DNA match alone. For example, in the UK this requirement is contained in Crown Prosecution Service Guidelines.[160] The UK Crown Prosecution Service has also produced guidance on the use of expert evidence, which includes DNA.[161]

Training of professionals, including law enforcement and court officers, is also important in ensuring fair trials and preventing miscarriages of justice. For example, US Federal law provides for training[162]:
"*(a) In general*
The Attorney General shall make grants to provide training, technical assistance, education, and information relating to the identification, collection, preservation, analysis, and use of DNA samples and DNA evidence by—
(1) law enforcement personnel, including police officers and other first responders, evidence technicians, investigators, and others who collect or examine evidence of crime;
(2) court officers, including State and local prosecutors, defense lawyers, and judges;
(3) forensic science professionals; and
(4) corrections personnel, including prison and jail personnel, and probation, parole, and other officers involved in supervision.
(b) Authorization of appropriations
There are authorized to be appropriated $12,500,000 for each of fiscal years 2015 through 2019 to carry out this section".

There is room for improvement in education and training in forensic genetics, even in European countries.[163] Ensuring access to justice may be more difficult in countries where the courts have limited resources.[164]

It is important that both prosecution and defence have equal access to forensic evidence.

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*States should ensure that DNA analysis as a specific means of proof is equally accessible to the defence, either by decision of a judicial authority or through the use of an independent expert.*
Where the quantity of substances available for analysis is limited, care should be taken to ensure that the rights of the defence are not impaired".[165]

5.2. Access to DNA evidence in the event of an appeal

Individuals should have a right to obtain re-analysis of crime scene forensic evidence in the event of appeal against conviction. Best practice includes legal requirements to preserve crime scene evidence used to convict incarcerated individuals so that they can appeal on grounds of their innocence by having the crime scene DNA examined. In the USA, the Innocence Project has been involved in more than 300 "DNA exonerations" in which people who have been wrongfully convicted have been freed as a result of post-conviction DNA testing.[166]

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*Recourse to DNA analysis should be permissible in all appropriate cases, independent of the degree of seriousness of the offence*".[167]

Examples of the legislation which explicitly includes the right to post-conviction testing are given in Annex U.

6. Safeguards for the international sharing of DNA evidence

International data flows need to be managed in a way that protects the rights of citizens. However, there is no universally agreed mechanism to do this[168]. For example, the Prüm system for automatic DNA database searches and sharing of DNA matches within the EU has led to significant controversy.[169,170,171,172,173,174, 175,176] Although this system contains some privacy protections, it has been criticised for: (1) the undemocratic way it was adopted; (2) inadequate safeguards to prevent large numbers of false ("adventitious") matches (which may divert resources and potentially lead to miscarriages of justice); (3) lack of adequate oversight and transparency; (4) its cost; and (5) failing to justify all the cross-border searches as necessary and proportionate to the need to tackle crime. Although cross-border crime certainly occurs, and in some cases cross-border DNA matches may be relevant to solving it, evidence to date suggests that a significant proportion of such crime may be relatively localised across neighbouring borders.[177,178] Concerns have also been raised about whether all EU member states have sufficient safeguards within their criminal justice systems to prevent miscarriages of justice: for example to prevent crime scene contamination and require corroborating evidence.[179] Bilateral agreements allowing the sharing of DNA and fingerprint matches have also been signed between a number of national governments and the United States.[180]

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*DNA analysis may be obtained from a laboratory or institution established in another country provided that the laboratory or institution satisfies all the requirements laid down in this recommendation.*
Transborder communication of the conclusions of DNA analysis should only be carried out between states complying with the provisions of this recommendation and in particular in accordance with the relevant international treaties on exchange of information in criminal matters and with Article 12 of the Data Protection Convention".[181]

UN Resolution 45/95 (Guidelines for the Regulation of Computerized Personal Data Files) states[182]:
"*9.* ***Transborder data flows***
When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely

as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands."

Best practice requires the provisions of relevant safeguards in both countries involved. In particular, data should be transferred overseas only when it is necessary and proportionate to do so, for the purpose for which it was originally collected, and the best practice standards outlined in this report must apply in both countries. For example, if a person's DNA profile is required to be deleted in the country of origin if they are acquitted, or after a certain period of time, this must also be required in the receiving one. Each party needs to implement and harmonise its national legislation in order to comply with international standards and so make possible and secure the international sharing of DNA profiles.

Examples are given in Annex V.

7. Relevant safeguards must be prescribed by law and there should be appropriate penalties for abuse

UN Resolution 45/95 (Guidelines for the Regulation of Computerized Personal Data Files) states[183]:
"*8. Supervision and sanctions*
The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies".

Council of Europe Recommendation No. R(92)1 on the use of analysis of DNA within the criminal justice system states: "*The establishment and operation of any DNA file for purposes of the investigation and prosecution of criminal offences should be regulated by law*".[184]

Including the safeguards described above in legislation can increase public confidence that DNA databases will operate lawfully and in a way that does not compromise individuals' human rights.

The law should be succinct and clear and cover all the relevant issues described above, and there must be adequate public and regulatory scrutiny to ensure it is working as intended (see Section 4.3). There should be no unregulated forensic DNA databases (for example, at state or local level, or held by commercial companies).

Proper public consultation is necessary from the outset when new legislation is being developed. For example, in the UK, Scotland held a public consultation about whether to follow the law introduced in England and Wales to allow indefinite retention of innocent people's DNA, and decided against doing this. As a result, Scotland avoided the controversy caused by the retention of innocent people's DNA in England and Wales, and the judgment against the UK Government in the 2008 Marper case at the European Court of Human Rights. In India, consultation on a new draft DNA Bill was initially resisted, leading to controversy: however, the Government then made a welcome decision to hold a public consultation.[185]

Examples of penalties included in DNA legislation are given in Annex W.

8. Police access to genetic databases established for non-criminal purposes

The scope of this report is limited to forensic DNA databases: we do not discuss in detail all the safeguards that should apply to stored DNA samples or databases where genetic information is collected and stored for other purposes. Such databases can include genetic information collected for health purposes, medical research, or to provide a commercial service such as providing information on paternity or genetic ancestry. In some databases, information or samples may be included from children, including babies (for example, when blood spots are collected at birth for health tests), or other vulnerable persons (such as mentally ill patients in a research project).

Nevertheless, in the context of this report, it is important to consider under what circumstances information in non-criminal genetic databases might be used in a criminal investigation and accessed by the police. In the UK, for example, a court order can be granted allowing police access to stored DNA samples and/or genetic information in any database.[186] In the USA, there have been some contentious cases where police have sought and gained access to genetic information, including one where an individual was falsely accused of an offence as a result of a 'familial search' of a commercial database.[187] If storage of genetic information for non-police purposes were to become widespread, and police access, including familial searching, widely used, in effect any individual and their relatives could be tracked using their DNA, undermining all the safeguards for forensic DNA databases highlighted above.

The Council of Europe's Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research states[188]:
"*Article 25 – Confidentiality*

1. *Any information of a personal nature collected during biomedical research shall be considered as confidential and treated according to the rules relating to the protection of private life.*
2. *The law shall protect against inappropriate disclosure of any other information related to a research project that has been submitted to an ethics committee in compliance with this Protocol*".

However, Council of Europe Recommendation No. R (97) 5 on the Protection of Medical Data states[189]:
"*7.3. Medical data may be communicated if they are relevant and:*
a. if the communication is provided for by law and constitutes a necessary measure in a democratic society for:
i. public health reasons; or
ii. the prevention of a real danger or the suppression of a specific criminal offence; or
iii. another important public interest; or
iv. the protection of the rights and freedoms of others; or
b. if the communication is permitted by law for the purpose of:
i. the protection of the data subject or a relative in the genetic line;
ii. safeguarding the vital interests of the data subject or a third person; or
iii. the fulfilment of specific contractual obligations; or
iv. establishing, exercising or defending a legal claim; or
c. if the data subject or his/her legal representative, or an authority, or any person or body provided for by law has given his/her consent for one or more purposes, and in so far as domestic law does not provide otherwise; or
d. provided that the data subject or his/her legal representative, or an authority, or any person or body provided for by law has not explicitly objected to any non-mandatory communication, if the

data have been collected in a freely chosen preventive, diagnostic or therapeutic context, and if the purpose of the communication, in particular the provision of care to the patient or the management of a medical service operating in the interest of the patient, is not incompatible with the purpose of the processing for which they were collected".

Thus, in Council of Europe member states, sharing genetic data stored for medical or research purposes with the police for criminal investigations should only take place with specific consent or for "*the prevention of a real danger or the suppression of a specific criminal offence*". However, no detail is provided on how such decisions should be made.

In relation to commercial databases, the private sector view is that[190]:

- the private sector should not be treated as an agent for law enforcement or surveillance - requests for assistance should be minimal and subject to strong oversight and conditions;
- the private sector should be free to disclose the nature and extent of government and law enforcement requests for access to data.

Best practice for police access to stored genetic information therefore requires strict oversight: including not only authorisation by a court, but also carefully defined guidance on the circumstances in which such requests can be granted, and how much data can be revealed. Further, information needs to be provided to people who take part in such databases so they are aware that police access could be granted, and information about the numbers and purposes of requests that are made and granted should be made available for public scrutiny.

9. Resources and priorities must be considered at the outset

Countries are often encouraged to embark on ambitious DNA database projects without considering the resources needed. Implementation of DNA databases in countries with new laws, but which lack existing forensic capacity, has generally been slow, due to the high costs and lack of existing infrastructure. Examples are South Africa and Brazil, which adopted legislation in 2012 and 2013, respectively, but have collected only relatively small numbers of DNA profiles to date.

Lobbyists can provide an exaggerated view of the potential benefits of DNA databases. For example, in Brazil, lobbyists from Gordon Thomas Honeywell, acting for the DNA testing industry, claimed that 3,000 stranger rapes a year are solved using the UK DNA database.[191] In reality, there were 29,265 rapes recorded by the police in England and Wales[192] in 2014-15, but only 192 of these led to matches on the DNA database with outcomes counted by the police (these include cases that have gone to court, but also cases where there are difficulties with evidence and the case does not go to court).[193] Not all of the matches will have identified a stranger who committed a rape: in many cases they confirm intercourse with a man who has already been identified by the victim, where the DNA database does not play an important role. And not all these suspects will be convicted if the suspect claims that intercourse was consensual. An estimated 5% to 25% of rapes may be stranger rapes[194]. So, in reality, only a handful of stranger rapes a year are likely to be solved using the UK DNA database, despite it being the largest DNA database per head of population in the world. In total, 8.5% of reported rape cases went to court in 2014/15 (2,488 cases), so the DNA database plays a relatively small role.[195]

As noted in Section 3.1, collection of DNA from crime scenes is far more important in driving the number of crimes solved than collection and storage of DNA profiles from large numbers of individuals. Stored crime scene DNA profiles can also play an important role in police intelligence by

linking crime scenes and revealing the behaviour of serial offenders: this information may also be of value in criminological research.[196,197] Most crimes solved using DNA do not require a DNA database of DNA profiles collected from known individuals: they require only crime scene DNA and DNA from known suspects for the crime. Using DNA effectively during criminal investigations requires proper crime scene examination in a context of trained and reliable policing, a trusted chain of custody of samples, reliable analysis, and proper use of expert evidence in court. Without these prerequisites, a DNA database will exacerbate rather than solve problems in the criminal justice system: for example, by leading to miscarriages of justice through false matches or misinterpretation or planting of evidence, and diverting resources from more important priorities.

In addition to the costs of establishing and maintaining them, DNA databases require a significant amount of police resources in order to identify, localise, and arrest individuals of interest, lay charges against them and ultimately commit them to trial. If the management of the database (e.g. types of cases to attend, individuals to include in the database) is not integrated within a clear policing strategy, police resources will be absorbed by certain types of crimes and individuals which are not necessarily in line with policing and security priorities.[198] This side effect becomes particularly evident when considering large and expanding databases and cross-border searches. For instance, the growth and networking of DNA databases at an international level will potentially multiply hits, in particular false positives, which may divert resources from other policing priorities (see Section 6).

Collecting and analysing large numbers of samples from persons who have no known connection to a crime is expensive, as is maintaining large databases. DNA databases that focus on collecting and storing crime scene evidence and DNA profiles from a more targeted population of known criminals, at high risk of reoffending, are more likely to be successfully implemented and to be cost-effective.

Detailed analysis of costs and a realistic appraisal of potential benefits are therefore needed before policies are adopted to set up or significantly expand DNA databases.

References

[1] Williams R, Wienroth M (2017) Social and ethical aspects of forensic genetics: A critical review. *Forensic Sci Rev* **29**, 145–169.

[2] Wallace, H (2012). A nova base de dados de DNA brasileira: solução de crimes ou erosão de direitos humanos? Revista Politics, 13ª Edição. Setembro, 2012. https://www.politics.org.br/categoria/politics-13

[3] Williams, R., Johnson, P., 2004. Circuits of Surveillance. *Surveill Soc* **2**, 1–14. doi:10.1901/jaba.2004.2-1

[4] For example, in Kuwait: http://dnapolicyinitiative.org/wiki/index.php?title=Kuwait and Portugal: Machado H, Silva S (2015) Public Perspectives on Risks and Benefits of Forensic DNA Databases: An Approach to the Influence of Professional Group, Education, and Age. *Bulletin of Science, Technology & Society* **35**, 16–24. doi:10.1177/0270467615616297

[5] Thompson WC. *The Potential for Error in Forensic DNA Testing (and How That Complicates the Use of DNA Databases for Criminal Identification)*. Council for Responsible Genetics Conference. Forensic DNA Databases and Race: Issues, Abuses and Actions. June 19-20, 2008, New York University. http://www.councilforresponsiblegenetics.org/pageDocuments/H4T5EOYUZI.pdf

[6] UNESCO (2003). International Declaration on Human Genetic Data. 16 October 2003. http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/human-genetic-data/

[7] United Nations (1948). The Universal Declaration on Human Rights. http://www.un.org/en/universal-declaration-human-rights/

[8] The United Nations Convention on the Rights of the Child. http://www.unicef.org.uk/Documents/Publication-pdfs/UNCRC_PRESS200910web.pdf

[9] DNA databases and human rights. GeneWatch UK briefing. January 2011. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/infopack_fin.pdf

[10] Algee-Hewitt BFB, Edge MD, Kim J, Li JZ, Rosenberg NA (2016) Individual Identifiability Predicts Population Identifiability in Forensic Microsatellite Markers. *Curr. Biol.* **26**, 935–942.

[11] Williams R, Johnson P, Martin P (2004) Genetic Information & Crime Investigation. ISBN 0 903 593 19 X http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=95F7E8031FDD63C04BEEAB23312B86F8?doi=10.1.1.670.4154&rep=rep1&type=pdf

[12] Washington, H (2010) Basic assumptions? Racial aspects of US DNA forensics. In: Hindmarsh, R. and Prainsack, B (2010) Genetic suspects: Global governance of forensic DNA profiling and databasing. Cambridge University Press.

[13] UN Resolution 45/95. Guidelines for the Regulation of Computerized Personal Data Files. E/CN.4/1990/72. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement

[14] OECD Privacy Principles. http://oecdprivacy.org/#principles

[15] WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects. http://www.wma.net/en/30publications/10policies/b3/

[16] UNESCO (1997) Universal Declaration on the Human Genome and Human Rights. 11 November 1997. http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/human-genome-and-human-rights/

[17] UNESCO (2006) Universal Declaration on Bioethics and Human Rights. http://unesdoc.unesco.org/images/0014/001461/146180e.pdf

[18] Krimsky, S, Simoncelli, T (2011) Genetic Justice: DNA data banks, criminal investigations, and civil liberties. Columbia University Press, New York.

[19] Directive (EU) 2016/680. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

[20] NDNAD Ethics Group: annual report 2008, Paragraph 5.4: http://www.homeoffice.gov.uk/publications/agencies-public-bodies/fsr/NDNAD_Ethics_Group_Annual_Report?view=Binary

[21] UK Home Office (2013) Biennial report 2009 to 2011: National DNA Database. Paragraph 2.9. https://www.gov.uk/government/publications/ndnad-biennial-report-2009-to-2011

[22] UNESCO (1997) Universal Declaration on the Human Genome and Human Rights. 11 November 1997. http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/human-genome-and-human-rights/

[23] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[24] Krimsky, S, Simoncelli, T (2011) Genetic Justice: DNA data banks, criminal investigations, and civil liberties. Columbia University Press, New York.

[25] Supreme Court of the United States. Maryland V. King. Certiorari to the Court of Appeals of Maryland No. 12–207. Argued February 26, 2013—Decided June 3, 2013. https://www.supremecourt.gov/opinions/12pdf/12-207_d18e.pdf

[26] State v. Medina (Vt. 2014) 102 A.3d 661, 663. http://legislature.vermont.gov/assets/Documents/2018/WorkGroups/House%20Judiciary/Bills/H.422/W~John%20Treadwell~State%20v%20Medina~3-14-2017.pdf

[27] Police 'arrest innocent youths for their DNA', officer claims. The Telegraph. 4th June 2009. http://www.telegraph.co.uk/news/uknews/law-and-order/5444332/Police-arrest-innocent-youths-for-their-DNA-officer-claims.html

[28] Arrested in O.C.? A DNA sample could buy freedom. Los Angeles Times. 17th September 2009. http://articles.latimes.com/2009/sep/17/local/me-oc-dna17

[29] A 12-year old-schoolboy arrested for allegedly stealing a pack of Pokemon cards. From schoolboy squabble to DNA database in one easy step - if you're black. The Times. 24th November 2009. http://www.timesonline.co.uk/tol/news/uk/crime/article6929014.ece
[30] Grandmother arrested for stealing football 'for revenge'. The Daily Mail. 5th October 2006. http://www.dailymail.co.uk/news/article-408819/Grandmother-arrested-stealing-football-revenge.html
[31] Fingerprinted and checked for DNA...the ten-year-old 'bullying victim'. The Evening Standard. 11th September 2009. http://www.thisislondon.co.uk/news/article-23366449-fingerprinted-and-checked-for-dnathe-ten-year-old-bullying-victim.do
[32] Arrested and DNA tested - for jokingly pinging a bra. The Daily Mail. 28th July 2006. http://www.dailymail.co.uk/news/article-398002/Arrested-DNA-tested--jokingly-pinging-bra.html
[33] Litter lout DNA samples a step too far. The Telegraph. 2nd August 2007. http://www.telegraph.co.uk/news/uknews/1559185/Litter-lout-DNA-samples-a-step-too-far.html
[34] Nature [Editorial] Genome abuse. Citizens are right to resist government pressure to expand population DNA databases. 27th September 2007. http://www.nature.com/nature/journal/v449/n7161/full/449377b.html
[35] Stop, armed police! Put down your MP3 player. The Guardian. 13th February 2008. http://www.guardian.co.uk/uk/2008/feb/13/ukguns.police
[36] Teen arrested by Southport police for handing in phone. Crosby Herald. 2nd April 2009. http://www.crosbyherald.co.uk/news/crosby-news/2009/04/02/teenager-arrested-by-southport-police-for-handing-in-mobile-phone-68459-23291295/
[37] BBC: Europe DNA ruling resonates in UK. 4th December 2008. http://news.bbc.co.uk/1/hi/uk/7765484.stm
[38] CASE OF S. AND MARPER v. THE UNITED KINGDOM. http://hudoc.echr.coe.int/eng?i=001-90051#{%22itemid%22:[%22001-90051%22]}
[39] Home Office (2013) NATIONAL DNA DATABASE STRATEGY BOARD ANNUAL REPORT 2012-13. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/252885/NDNAD_Annual_Report_2012-13.pdf
[40] Wallace HM, Jackson AR, Gruber J, Thibedeau AD (2014). Forensic DNA databases - Ethical and legal standards: A global review. *Egyptian Journal of Forensic Sciences*, **4**(3), 57–63. http://www.sciencedirect.com/science/article/pii/S2090536X14000239
[41] Home Office (2014) National DNA Database: annual report, 2013 to 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/387581/NationalDNAdatabase201314.pdf
[42] Krimsky, S, Simoncelli, T (2011) Genetic Justice: DNA data banks, criminal investigations, and civil liberties. Columbia University Press, New York.
[43] Krimsky, S, Simoncelli, T (2011) Genetic Justice: DNA data banks, criminal investigations, and civil liberties. Columbia University Press, New York.
[44] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2
[45] DNA database 'is causing suicides', MPs are warned. Daily Mail. 4th February 2010. http://www.dailymail.co.uk/news/article-1248358/DNA-database-causing-suicides-MP-warned.html
[46] 'Orwellian' CCTV in shires alarms senior police officer. The Guardian. 21st May 2007. http://www.guardian.co.uk/uk/2007/may/21/ukcrime.humanrights
[47] A simple prank by a 13-year-old. Now her genetic records are on the National DNA Database for ever New Statesman. 25th April 2005. http://www.newstatesman.com/200504250026
[48] Innocent 'terror techie' purges DNA records The Register. 17th September 2007. http://www.theregister.co.uk/2007/09/17/dna_purge/
[49] Janet Street-Porter: I'm innocent. So the police have no right to keep my DNA on file. The Independent. 31st July 2008. http://www.independent.co.uk/opinion/columnists/janet-street-porter/janet-streetporter-im-innocent-so-the-police-have-no-right-to-keep-my-dna-on-file-881272.html
[50] Comedian Mark Thomas. How I got my genes deleted. The Guardian. 19th March 2009. http://www.guardian.co.uk/commentisfree/2009/mar/19/dna-database-comment

[51] Tory MP demands return of DNA sample as decision not to press charges leaves ministers red-faced but police in clear. DPP's verdict on papers leaked in Damian Green affair - Not a threat to security. The Guardian. 17th April 2009. http://www.guardian.co.uk/politics/2009/apr/17/damian-green-arrest-jacqui-smith

[52] Remove my DNA sample from government files, demands MP. Daily Mail. 3rd August 2008. http://www.dailymail.co.uk/news/article-1041267/Remove-DNA-sample-government-files-demands-MP.html

[53] DNA of one-year-old baby stored on national database. The Telegraph. 10th March 2009. http://www.telegraph.co.uk/news/politics/4966168/DNA-of-one-year-old-baby-stored-on-national-database.html

[54] Learning to live with Big Brother. The Economist. 27th September 2007. http://www.economist.com/node/9867324?story_id=9867324

[55] Police retain DNA of 'petty crime suspects'. The Telegraph. 4th November 2007. http://www.telegraph.co.uk/news/uknews/1568269/Police-retain-DNA-of-petty-crime-suspects.html

[56] Black church leaders concerned over criminal DNA database. Christian Today. 18th July 2008. http://www.christiantoday.com/article/black.church.leaders.concerned.over.criminal.dna.database/20635.htm

[57] Wallace HM, Jackson AR, Gruber J, Thibedeau AD (2014). Forensic DNA databases - Ethical and legal standards: A global review. *Egyptian Journal of Forensic Sciences*, **4**(3), 57–63. https://doi.org/10.1016/j.ejfs.2014.04.002

[58] Home Office (2013) National DNA Database Strategy Board Annual Report 2012-13. https://www.gov.uk/government/publications/national-dna-database-annual-report-2012-to-2013

[59] UK Home Office. National DNA Database: annual report, 2013 to 2014; National DNA Database: annual report, 2014 to 2015; National DNA Database: annual report, 2015 to 2016. Available on: https://www.gov.uk/government/collections/dna-database-documents

[60] UN Resolution 45/95. Guidelines for the Regulation of Computerized Personal Data Files. E/CN.4/1990/72. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement

[61] Directive (EU) 2016/680. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

[62] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[63] OECD Privacy Principles. http://oecdprivacy.org/#principles

[64] Directive (EU) 2016/680. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

[65] LEI Nº 9.507, DE 12 DE NOVEMBRO DE 1997. http://www.planalto.gov.br/ccivil_03/leis/L9507.htm

[66] Guadamuz A (2001) Habeas Data vs the European Data Protection Directive. *Journal of Information Law & Technology* 2001(3). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz

[67] https://www.nacro.org.uk/resettlement-advice-service/support-for-practitioners/criminal-record-checks/#nfa

[68] https://uk.usembassy.gov/visas/ineligibilities-and-waivers-2/arrest-caution-conviction/

[69] European Court of Human Rights (2011) Dimitrov-Kazakov v. Bulgaria (no. 11379/03). Press Release issued by the Registrar of the Court no. 121. 10th February 2011. https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwijye32g6fUAhXlA8AKHRSUCGsQFggpMAA&url=http%3A%2F%2Fhudoc.echr.coe.int%2Fapp%2Fconversion%2Fpdf%2F%3Flibrary%3DECHR%26id%3D003-3432320-3856698%26filename%3D003-3432320-3856698.pdf&usg=AFQjCNGU05HpCkL6H4Lv4ETEjrqaRJcNGg

[70] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[71] Protection of Freedoms Act 2012. Section 9. http://www.legislation.gov.uk/ukpga/2012/9/section/9/enacted

[72] Protection of Freedoms Act 2012. Section 20. http://www.legislation.gov.uk/ukpga/2012/9/section/20/enacted

[73] Protection of Freedoms Act 2012. Section 21. http://www.legislation.gov.uk/ukpga/2012/9/section/21/enacted

[74] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[75] UN Resolution 45/95. Guidelines for the Regulation of Computerized Personal Data Files. E/CN.4/1990/72. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement

[76] OECD Privacy Principles. http://oecdprivacy.org/#principles

[77] Risher MT (2011) Racial disparities in databanking of DNA profiles. In: Race and the genetic revolution. Krimsky S, Sloan K (Eds). Columbia University Press.

[78] Wallace HM (2011) Prejudice, stigma and DNA databases. In: Race and the genetic revolution. Krimsky S, Sloan K (Eds). Columbia University Press.

[79] UN Resolution 45/95. Guidelines for the Regulation of Computerized Personal Data Files. E/CN.4/1990/72. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement

[80] Directive (EU) 2016/680. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

[81] Ribaux O, Baylon A, Roux C, Delémont O, Lock E, Zingg C, Margot P (2010) Intelligence-led crime scene processing. Part I: Forensic intelligence. *Forensic Sci. Int.* **195**, 10–16. doi:10.1016/j.forsciint.2009.10.027

[82] Wallace HM, Jackson AR, Gruber J, Thibedeau AD (2014) Forensic DNA databases–Ethical and legal standards: A global review. *Egyptian Journal of Forensic Sciences*, **4**(3), 57–63. http://doi.org/10.1016/j.ejfs.2014.04.002

[83] Samuels JE, Davies EH, Pope DB. Collecting DNA at arrest: policies, practices, and implications. The Urban Institute. Final Technical Report. Washington, May 2013. http://www.urban.org/UploadedPDF/412831-Collecting-DNA-at-Arrest-Policies-Practices-and-Implications-Report.pdf

[84] Rape in America: Justice Denied. CBS News. 9th November 2009. http://www.cbsnews.com/news/exclusive-rape-in-america-justice-denied/

[85] http://www.endthebacklog.org/

[86] 10,000 Backlogged Rape Kits Finally Tested Lead to Hundreds of Indictments in Ohio. AllGov. 22nd February 2016. http://www.allgov.com/news/unusual-news/10000-backlogged-rape-kits-finally-tested-lead-to-hundreds-of-indictments-in-ohio-160222?news=858347

[87] Thompson WC. *The Potential for Error in Forensic DNA Testing (and How That Complicates the Use of DNA Databases for Criminal Identification)*. Council for Responsible Genetics Conference. Forensic DNA Databases and Race: Issues, Abuses and Actions. June 19-20, 2008, New York University. http://www.councilforresponsiblegenetics.org/pageDocuments/H4T5EOYUZI.pdf

[88] How DNA Evidence Incriminated an Impossible Suspect, New Republic. 26th October 2015. https://newrepublic.com/article/123177/how-dna-evidence-incriminated-impossible-suspect

[89] Forensic Regulator (2015) The Control and Avoidance of Contamination in Crime Scene Examination involving DNA Evidence Recovery FSR-G-206.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/393866/206_FSR_SOC_contamination_consultation.pdf

[90] Carracedo Á, Miguel AM (2017) A state-of-the-art description of handling biological evidence from crime scene to court room. The European Forensic Genetics Network of Excellence (EUROFORGEN-NoE). https://www.euroforgen.eu/fileadmin/websites/euroforgen/images/Dissemination_Documents/EUROFORGEN-NoE_State-of-the-art_2014.pdf

[91] Forensic Regulator (2015) The Control and Avoidance of Contamination In Crime Scene Examination involving DNA Evidence Recovery FSR-G-206. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/393866/206_FSR_SOC_contamination_consultation.pdf

[92] Technical Working Group on Biological Evidence Preservation. The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers. NISTIR 7928. http://www.nist.gov/forensics/upload/NIST-IR-7928.pdf

[93] Understaffed and abysmal: India's police story in numbers. CatchNews. 14th February 2017. http://www.catchnews.com/india-news/understaffed-and-abysmal-india-s-police-story-in-numbers-1453642129.html

[94] Maguire ER, King WR (2013) Transferring criminal investigation methods from developed to developing nations. *Policing and Society* **23**, 346–361.

[95] https://www.gov.uk/government/organisations/forensic-science-regulator

[96] Available on: http://www.criminaljustice.ny.gov/forensic/aboutofs.htm . Accessed 10/04/14.

[97] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[98] Thompson WC. *The Potential for Error in Forensic DNA Testing (and How That Complicates the Use of DNA Databases for Criminal Identification)*. Council for Responsible Genetics Conference. Forensic DNA Databases and Race: Issues, Abuses and Actions. June 19-20, 2008, New York University. http://www.councilforresponsiblegenetics.org/pageDocuments/H4T5EOYUZI.pdf

[99] Hundreds of DNA Samples May Need Retesting. Time Warner Cable News. 21st October 2015. http://www.twcnews.com/tx/austin/news/2015/10/21/hundreds-of-dna-samples-may-need-retesting.html

[100] GC of Forensic Science Commission Focuses on Collaboration. Texas Lawyer. 2nd November 2015. http://www.texaslawyer.com/id=1202741043367/GC-of-Forensic-Science-Commission-Focuses-on-Collaboration?mcode=0&curindex=0&curpage=ALL&slreturn=20151017103546

[101] FBI Errors Lead to Discovery that DNA Evidence May be Far Less Foolproof When It Includes More than One Person. AllGov. 10th September 2015. http://www.allgov.com/news/unusual-news/fbi-errors-lead-to-discovery-that-dna-evidence-may-be-far-less-foolproof-when-it-includes-more-than-one-person-150910?news=857388

[102] DNA database in doubt after teenager spends three months behind bars for rape in city he has never even visited because gene samples were mixed up. Daily Mail. 18th May 2012. http://www.dailymail.co.uk/news/article-2114252/Teenager-spends-months-bars-DNA-blunder-fingers-rape-city-visited.html

[103] Las Vegas police reveal DNA error put wrong man in prison. Las Vegas Review Journal. 7th July 2011. http://www.reviewjournal.com/news/crime-courts/las-vegas-police-reveal-dna-error-put-wrong-man-prison

[104] DNA Testing: Foolproof? CBS News. 11th February 2009. http://www.cbsnews.com/news/dna-testing-foolproof/

[105] DNA Match Tying Protest to 2004 Killing Is Doubted. The New York Times. 11th July 2012. http://www.nytimes.com/2012/07/12/nyregion/suspected-dna-link-to-2004-killing-was-the-result-of-a-lab-error.html

[106] Cleared murder accused victim of DNA blunder. Liverpool Daily Post. 10th March 2003. http://www.liverpoolecho.co.uk/news/?objectid=12718961&method=full&siteid=50061

[107] Poor infra in forensic labs cripples fight. Times of India. 21st September 2016. http://timesofindia.indiatimes.com/city/delhi/Poor-infra-in-forensic-labs-cripples-fight/articleshow/54434290.cms

[108] Delhi forensic lab accused of filing false reports, framing innocents. Hindustan Times. 3rd March 2016. http://www.hindustantimes.com/delhi/delhi-forensic-lab-accused-of-filing-false-reports-framing-innocents/story-6NhLWt372aHERFWd4ufTKO.html

[109] Could better DNA testing facilities in India have saved the Talwars? First Post. 11th October 2012. http://www.firstpost.com/india/could-better-dna-testing-facilities-in-india-have-saved-the-talwars-486172.html

[110] New forensic science service planned. BBC. 12th March 2016. http://www.bbc.co.uk/news/uk-35793073

[111] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[112] Ge, J, Eisenberg, A, Budowle, B (2012) Developing criteria and data to determine best options for expanding the core CODIS loci. *Investigative Genetics*, **3**:1. http://www.investigativegenetics.com/content/3/1/1

[113] Buckleton J, Triggs CM (2005). Relatedness and DNA: are we taking it seriously enough? *Forensic Science International*, **152**(2-3), 115–119. http://doi.org/10.1016/j.forsciint.2004.07.020

[114] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[115] DNA test put on trial. Times Union. 16th September 2013. http://www.timesunion.com/local/article/DNA-test-put-on-trial-4815368.php

[116] Reliability Questions Raised Over Algorithm Analysis of Murky DNA Evidence in Criminal Cases. AllGov. 5th November 2016. http://www.allgov.com/news/controversies/reliability-questions-raised-over-algorithm-analysis-of-murky-dna-evidence-in-criminal-cases-161105?news=859721

[117] UK Forensic Science Regulator (2014). Protocol: DNA contamination detection – The management and use of staff elimination DNA databases. FSR-P-302. ISSUE 1. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/355995/DNAcontaminationDetection.pdf

[118] Butler J (2012) Advanced topics in forensic DNA typing: methodology. London: Elsevier, pp 228-229.

[119] Police Released a Suspect Photo Based on DNA From a Decades-Old Murder. Motherboard. 26th January 2017. https://motherboard.vice.com/en_us/article/police-released-a-suspect-photo-based-on-dna-from-a-decades-old-murder

[120] Library of Parliament (Canada), Parliamentary Information and Research Service (2009) New Frontiers in Forensic DNA Analysis: Implications for Canada's National DNA Data Bank (March 3, 2009: PRB 08-29E). http://www.lop.parl.gc.ca/content/lop/researchpublications/prb0829-e.pdf

[121] STS@Freiburg. Open Letter. 8th December 2016. https://stsfreiburg.wordpress.com/english/open-letter/

[122] Night Stalker: police blunders delayed arrest of Delroy Grant.The Telegraph. 24th March 2001. http://www.telegraph.co.uk/news/uknews/crime/8397585/Night-Stalker-police-blunders-delayed-arrest-of-Delroy-Grant.html

[123] National DNA Database Ethics Group (2017) Next generation sequencing technologies: ethical considerations. https://www.gov.uk/government/publications/next-generation-sequencing-technologies-ethical-considerations

[124] Hindmarsh R, Prainsack, B (2010) Genetic suspects: Global governance of forensic DNA profiling and databasing. Cambridge University Press.

[125] OECD Privacy Principles. http://oecdprivacy.org/#principles

[126] The forensic use of bioinformation: ethical issues. Nuffield Council on Bioethics. London. September 2007. http://nuffieldbioethics.org/wp-content/uploads/The-forensic-use-of-bioinformation-ethical-issues.pdf

[127] Toom, V (2012). Forensic DNA databases in England and the Netherlands: governance, structure and performance compared. *New Genetics and Society*, **31**(3), 311–322.

[128] https://www.gov.uk/government/publications/national-dna-database-strategy-board-governance-rules

[129] https://www.gov.uk/government/organisations/national-dna-database-ethics-group

[130] https://www.gov.uk/government/organisations/biometrics-commissioner
[131] https://www.gov.uk/government/organisations/forensic-science-regulator
[132] https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/national-dna-database-delivery-unit/
[133] http://www.justica.gov.br/sua-seguranca/ribpg
[134] UNESCO (1997) Universal Declaration on the Human Genome and Human Rights. 11 November 1997. http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/human-genome-and-human-rights/
[135] Banisar D (2014) National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map. Article 19. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416
[136] Data Protection Global Guide. Practical Law. http://uk.practicallaw.com/resources/global-guides/dataprotection-guide
[137] UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. United Nations, Geneva. http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf
[138] UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. United Nations, Geneva. http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf
[139] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC
[140] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2
[141] COUNCIL OF EUROPE COMMITTEE OF MINISTERS RECOMMENDATION No. R (87) 15 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR 1 (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies). http://ec.europa.eu/justice/data-protection/law/files/coe-fra-rpt-2670-en-471.pdf
[142] Cannataci JA, Caruana MM (2013) Recommendation R (87) 15 – Twenty–five years down the line. Council of Europe. http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf
[143] OECD Privacy Principles. http://oecdprivacy.org/#principles
[144] 42 U.S. Code § 14132 - Index to facilitate law enforcement exchange of DNA identification information. https://www.law.cornell.edu/uscode/text/42/14132
[145] Privacy bill held up due to intel agency reservations. The New Indian Express. 7th March 2017. http://www.newindianexpress.com/nation/2017/mar/07/privacy-bill-held-up-due-to-intel-agency-reservations-1578461.html
[146] OECD Privacy Principles. http://oecdprivacy.org/#principles
[147] UN Resolution 45/95. Guidelines for the Regulation of Computerized Personal Data Files. E/CN.4/1990/72. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement
[148] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2
[149] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC
[150] Council of Europe Recommendation No. R (97) 5 on the Protection of Medical Data. 13th February, 1997. http://hrlibrary.umn.edu/instree/coerecr97-5.html

[151] UNESCO (1997) Universal Declaration on the Human Genome and Human Rights. 11 November 1997. http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/human-genome-and-human-rights/

[152] UNESCO (2003). International Declaration on Human Genetic Data. 16 October 2003. http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/human-genetic-data/

[153] Greely HT, Riordan DP, Garrison NA, Mountain JL (2006). Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin. *The Journal of Law, Medicine & Ethics*, **34**(2), 248–262. https://doi.org/10.1111/j.1748-720X.2006.00031.x

[154] Hicks T, Taroni F, Curran J, Buckleton J, Castella V, Ribaux O (2010). Use of DNA profiles for investigation using a simulated national DNA database: Part II. Statistical and ethical considerations on familial searching. *Forensic Science International*: *Genetics*, **4**(5), 316–322. https://doi.org/10.1016/j.fsigen.2009.11.006

[155] Rohlfs RV, Fullerton SM, Weir BS (2012) Familial identification: population structure and relationship distinguishability. *PLoS Genetics*, **8**(2), e1002469. https://doi.org/10.1371/journal.pgen.1002469

[156] Rohlfs RV, Murphy E, Song YS, Slatkin M. (2013) The Influence of Relatives on the Efficiency and Error Rate of Familial Searching. *PLoS ONE*, **8**(8), e70495. https://doi.org/10.1371/journal.pone.0070495

[157] Rothstein MA, Talbott MK (2006) The Expanding Use of DNA in Law Enforcement: What Role for Privacy? *The Journal of Law, Medicine & Ethics*, **34**(2), 153–164. https://doi.org/10.1111/j.1748-720X.2006.00024.x

[158] Williams R, Johnson P (2005) Inclusiveness, Effectiveness and Intrusiveness: Issues in the Developing Uses of DNA Profiling in Support of Criminal Investigations. *The Journal of Law, Medicine Ethics*: **33**(3), 545–558.

[159] Krimsky, S, Simoncelli, T (2011) Genetic Justice: DNA data banks, criminal investigations, and civil liberties. Columbia University Press, New York.

[160] Crown Prosecution Service: Guidance on DNA Charging. 16th July 2004. https://www.cps.gov.uk/legal/assets/uploads/files/pdf_000328%20-%20%20DNA%20Charging%20Guidance.pdf

[161] Crown Prosecution Service (2015) Expert Evidence. First edition – 2014 revised February 2015. http://www.cps.gov.uk/legal/assets/uploads/files/expert_evidence_first_edition_2014.pdf

[162] 42 U.S. Code § 14136 - DNA training and education for law enforcement, correctional personnel, and court officers. https://www.law.cornell.edu/uscode/text/42/14136

[163] Poulsen L, Morling N (2013) White Book on the current status of education and training in forensic genetics in Europe. March 2013. European Forensic Genetics Network of Excellence (EUROFORGEN-NoE). https://www.euroforgen.eu/fileadmin/websites/euroforgen/images/Training/White_book_final.pdf

[164] Examining the funding deficit of the judiciary. LiveMint. 15th December 2016. http://www.livemint.com/Opinion/b1DNafTIUNGtzY3IR8gtbI/Examining-the-funding-deficit-of-the-judiciary.html

[165] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[166] The Innocence Project. http://www.innocenceproject.org/

[167] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[168] UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. United Nations, Geneva. http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

[169] McCartney CI, Wilson TJ, Williams R (2011). Transnational Exchange of Forensic DNA: Viability, Legitimacy, and Acceptability. *European Journal on Criminal Policy and Research*, **17**(4), 305–322. https://doi.org/10.1007/s10610-011-9154-y

[170] Prainsack B, Toom V (2010) The Prüm Regime: Situated Dis/Empowerment in Transnational DNA Profile Exchange. *British Journal of Criminology*, **50**(6), 1117–1135. https://doi.org/10.1093/bjc/azq055

[171] Prainsack B, Toom V (2013) Performing the Union: the Prüm Decision and the European dream. *Studies in History and Philosophy of Biological and Biomedical Sciences*, **44**(1), 71–79. https://doi.org/10.1016/j.shpsc.2012.09.009

[172] Balzacq T, Hadfield A (2012) Differentiation and trust: Prüm and the institutional design of EU internal security. *Cooperation and Conflict* **47**, 539–561. doi:10.1177/0010836712462781

[173] McCartney C (2015) Forensic data exchange: ensuring integrity. *Australian Journal of Forensic Sciences* **47**, 36–48. doi:10.1080/00450618.2014.906654

[174] van der Beek CP (2011) Forensic DNA Profiles Crossing Borders in Europe (Implementation of the Treaty of Prüm) [WWW Document]. URL http://www.promega.co.uk/resources/profiles-in-dna/2011/forensic-dna-profiles-crossing-borders-in-europe/

[175] Schneider P (2009) Expansion of the European Standard Set of DNA Database Loci—the Current Situation. *Profiles in DNA* **12**, 6–7.

[176] Santos F, Machado H (2017) Patterns of exchange of forensic DNA data in the European Union through the Prüm system. *Science & Justice*. doi:10.1016/j.scijus.2017.04.001

[177] Taverne MD, Broeders APA (2017) Cross-border patterns in DNA matches between the Netherlands and Belgium. *Science & Justice* **57**, 28–34. doi:10.1016/j.scijus.2016.08.008

[178] Bernasco W, Lammers M, Beek K van der (2016) Cross-border crime patterns unveiled by exchange of DNA profiles in the European Union. *Secur J* **29**, 640–660. doi:10.1057/sj.2015.27

[179] Sharing DNA profiles and fingerprints across the EU requires further safeguards. GeneWatch UK Briefing. 2nd December 2015. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/Pruembrief_Nov15_fin.pdf

[180] Examples are available on: http://dnapolicyinitiative.org/wiki/index.php?title=International_resources

[181] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[182] UN Resolution 45/95. Guidelines for the Regulation of Computerized Personal Data Files. E/CN.4/1990/72. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement

[183] UN Resolution 45/95. Guidelines for the Regulation of Computerized Personal Data Files. E/CN.4/1990/72. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement

[184] COUNCIL OF EUROPE COMMITTEE OF MINISTERS (1992) RECOMMENDATION No. R (92) 1 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE USE OF ANALYSIS OF DEOXYRIBONUCLEIC ACID (DNA) WITHIN THE FRAMEWORK OF THE CRIMINAL JUSTICE SYSTEM (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies). https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2

[185] Government Invites Comments on DNA Profiling Bill, Even if Belatedly. The Wire. 18th August 2015. https://thewire.in/8698/government-invites-comments-on-dna-profiling-bill-even-if-belatedly/

[186] Kaye, J. (2006). Police Collection and Access to DNA Samples. *Genomics, Society and Policy*, **2**, 16–27.

[187] Ancestory firms' DNA database use suspect. The Clarion-Ledger. 27th March 2016. http://www.clarionledger.com/story/news/2016/03/27/ancestory-firms-dna-database-use-suspect/82329306/

[188] Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research. Council of Europe Treaty Series - No. 195. http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008371a

[189] Council of Europe Recommendation No. R (97) 5 on the Protection of Medical Data. 13th February, 1997. http://hrlibrary.umn.edu/instree/coerecr97-5.html

[190] UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. United Nations, Geneva. http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

[191] http://www.dnaresource.com/documents/BRAZILBrasiliaJuly2010(2).pdf

[192] Note: Scotland and Norther Ireland have separate DNA databases, and only export DNA profiles to the UK database when the crimes have not been solved.

[193] Table 4. National DNA Database Strategy Board Annual Report 2014/15. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/484937/52921_NPCC_National_DNA_Database_web_pdf.pdf

[194] Criminal Justice Joint Inspection (2012) Forging the links: Rape investigation and prosecution A joint review by HMIC and HMCPSI. February 2012. ISBN: 978-1-84987-688-9. http://www.hmic.gov.uk/media/forging-the-links-rape-investigation-and-prosecution-20120228.pdf

[195] Table 2.3. Crime Outcomes in England and Wales 2014/15. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445753/hosb0115.pdf

[196] Ribaux O, Baylon A, Roux C, Delémont O, Lock E, Zingg C, Margot P (2010) Intelligence-led crime scene processing. Part I: Forensic intelligence. *Forensic Sci. Int.* **195**, 10–16. doi:10.1016/j.forsciint.2009.10.027

[197] Moor SD, Beken TV, Daele SV (2016) DNA Databases as Alternative Data Sources for Criminological Research. *Eur J Crim Policy Res* 1–18. doi:10.1007/s10610-016-9327-9

[198] Ribaux O, Baylon A, Roux C, Delémont O, Lock E, Zingg C, Margot P (2010) Intelligence-led crime scene processing. Part I: Forensic intelligence. *Forensic Sci. Int.* **195**, 10–16. doi:10.1016/j.forsciint.2009.10.027

Annex A: Examples of Consent Requirements in DNA Database Legislation

The German Code of Criminal Procedure[199] states:
"*Section 81h [Serial Molecular and Genetic Examination]*
(1) Where certain facts give rise to the suspicion that a felony against life, physical integrity, personal freedom or sexual self-determination has been committed, then with their written consent, persons who manifest certain significant features which may be assumed to apply to the perpetrator 1. may have cell tissue collected from them which will be 2. subjected to a molecular and genetic examination to establish gender and the DNA profile, and 3. the DNA profiles established automatically matched against the DNA profiles of trace materials, insofar as this is necessary in order to ascertain whether the trace material(s) originated from such persons and the measure is not disproportionate to the gravity of the offence, particularly in view of the number of persons affected by the measure.
(2) Any measure pursuant to subsection (1) shall require a court order. This order shall be issued in writing. The order shall designate the persons concerned by reference to specified significant features and shall give reasons. A prior examination of the persons concerned shall not be required. The decision ordering the measure shall not be contestable.
(3) Sections 81f subsection (2) and Section 81g subsection (2) shall apply mutatis mutandis to the implementation of the measure. Insofar as the data relating to the DNA profiles established by the measure is no longer necessary for clearing up the felony it shall be deleted without delay. The fact of the deletion shall be documented.
(4) The persons concerned are to be instructed in writing that the measure may only be implemented with their consent. They are also to be instructed that
1. the cell tissue collected shall be used exclusively for the molecular and genetic examination pursuant to subsection (1) and shall be destroyed without delay once they are no longer required for this purpose, and 2. that the DNA profiles established shall not be stored by the Federal Criminal Police Office for the purposes of establishing identity in future criminal proceedings."

In Germany, the law on the data of DNA analysis states[200]:
"*(4) DNA identification patters that have been gained in the light of the data subject's consent, may only be stored in the file, if the person has given consent in regard to the inclusion in the BKA DNA analysis file".* (Section 2.2)

The Netherlands' Code of Criminal Procedure states[201]: "*Section 151a*
1. The public prosecutor may instruct, ex officio or on application of the suspect or his defence counsel, a third party to conduct DNA testing aimed at comparing DNA profiles in the interest of the investigation. He may request the suspect or a third party to provide cellular material for DNA testing. Except in the case of application of section 151lb or of a missing person as referred to in the last sentence, cellular material may only be taken with the written consent of the suspect or the third party. Cellular material shall be taken from the suspect only after one or more of the suspect's fingerprints have been taken and processed in accordance with this Code and his identity has been established in the manner referred to in section 27a(1, first sentence) and (2). A request for the provision of cellular material may be made to a group of fifteen third parties or more only with written authorisation granted by the examining magistrate on application of the public prosecutor. In the event that the third party is missing as a result of a serious offence, DNA testing may be

conducted on cellular material on objects seized from him or on cellular material obtained in another way."

US Federal law states[202]:
"*(a) Establishment of index*
The Director of the Federal Bureau of Investigation may establish an index of—
(1) DNA identification records of—
(A) persons convicted of crimes;
(B) persons who have been charged in an indictment or information with a crime; and
(C) other persons whose DNA samples are collected under applicable legal authorities, provided that DNA samples that are voluntarily submitted solely for elimination purposes shall not be included in the National DNA Index System;
(2) analyses of DNA samples recovered from crime scenes;
(3) analyses of DNA samples recovered from unidentified human remains; and
(4) analyses of DNA samples voluntarily contributed from relatives of missing persons".

Annex B: Examples of Legislative Provisions for Collection of DNA Without Consent

In many countries, the police require authorisation by a judge to take a DNA sample from an individual suspect. An example is Canada's law[203]:

"487.05 (1) A provincial court judge who on ex parte application is satisfied by information on oath that there are reasonable grounds to believe

(a) that a designated offence has been committed,

(b) that a bodily substance has been found

(i) at the place where the offence was committed,

(ii) on or within the body of the victim of the offence,

(iii) on anything worn or carried by the victim at the time when the offence was committed, or

(iv) on or within the body of any person or thing or at any place associated with the commission of the offence,

(c) that a person was a party to the offence, and

(d) that forensic DNA analysis of a bodily substance from the person will provide evidence about whether the bodily substance referred to in paragraph (b) was from that person

and who is satisfied that it is in the best interests of the administration of justice to do so may issue a warrant in writing authorizing a peace officer to obtain, or cause to be obtained under the direction of the peace officer, a bodily substance from that person, by means of an investigative procedure described in subsection 487.06(1), for the purpose of forensic DNA analysis.

Criteria

(2) In considering whether to issue the warrant, the provincial court judge shall have regard to all relevant matters, including

(a) the nature of the designated offence and the circumstances of its commission; and

(b) whether there is

(i) a peace officer who is able, by virtue of training or experience, to obtain a bodily substance from the person, by means of an investigative procedure described in subsection 487.06(1), or

(ii) another person who is able, by virtue of training or experience, to obtain under the direction of a peace officer a bodily substance from the person, by means of such an investigative procedure."

Argentina's law states[204]: "*the Records of Genetic Fingerprinting will be implemented as a database to record any genetic fingerprint associated with evidence from different crime scenes or clothing of the victims, or genetic profiles made in the course of judicial proceedings by order of the courts involved or prosecutors*".

The Republic of Korea's law states[205]:

"*Article 8 (Warrant to Collect DNA Samples)*

(1) A public prosecutor may collect DNA samples from a person subject to collection of DNA samples under Article 5 or 6 with a warrant issued by the competent district court judge (including a military judge; the same shall apply hereinafter) at the request of the public prosecutor.

(2) A judicial police officer may collect DNA samples from a person subject to collection of DNA samples under Article 6 with a warrant issued by the competent district court judge at the request of the public prosecutor with whom the judicial police officer files an application for the warrant.

(3) If a person subject to collection of DNA samples under paragraph (1) or (2) consents to the collection, DNA samples may be collected without a warrant. In such cases, a notice that the person may refuse the collection shall be given in advance, and consent thereto shall be obtained in writing.

(4) A request for a warrant to collect DNA samples under paragraph (1) or (2) (hereinafter referred to as "warrant to collect DNA samples") shall be made in writing, describing the name and address of the person subject to the collection, reasons for the request, types of samples to be collected, the

method and place of collection, etc. and shall be accompanied by documents supporting the reasons for the request.
(5) Each warrant to collect DNA samples shall contain the name and address of the person subject to the collection, types of samples to be collected, the method and place of collection, the effective period, and a statement that, if the effective period lapses, the warrant shall be unenforceable and thus shall be returned, and shall bear the signature and seal affixed by the competent district court judge.
(6) A warrant to collect DNA samples shall be executed by a judicial police officer under the competent public prosecutor's command: Provided, That a warrant to collect DNA samples of a person who is in the custody of a custody facility may be executed by a public official who works for the custody facility under the competent public prosecutor.
(7) A public prosecutor may directly command the execution of a warrant to collect DNA samples at a place outside his/her jurisdiction or entrust a public prosecutor having jurisdiction over the place with the command of execution.
(8) Whenever DNA samples are collected, a notice of grounds on which such DNA samples are collected, types of samples to be collected, and the method of collection shall be given in advance to the person subject to the collection.
(9) As to the collection of DNA samples with a warrant to collect DNA samples, Articles 116, 118, 124 through 126, and 131 of the Criminal Procedure Act shall apply mutatis mutandis."

The German Code of Criminal Procedure[206] states:
"*(3) Without the written consent of the person concerned, the collection of cell tissue may be ordered only by the court and, in exigent circumstances, by the public prosecution office including the officials assisting it (section 152 of the Courts Constitution Act). Without the written consent of the person concerned, the molecular and genetic examination of cell tissue may be ordered only by the court. Persons who have consented are to be instructed as to the purpose for which the data to be obtained will be used. Section 81f subsection (2) shall apply mutatis mutandis. In its written reasons the court shall specify in relation to the particular case concerned 1. the determining facts relevant to ascertaining the seriousness of the criminal offence, 2. the information giving rise to the assumption that the accused will be the subject of criminal proceedings in the future, as well as 3. an evaluation of the relevant circumstances in each case.*
(4) Subsections (1) to (3) shall apply mutatis mutandis if the person concerned has been convicted of the offence with binding effect or was not convicted merely on the grounds that 1. lack of criminal responsibility has been proven or cannot be ruled out, 2. he is unfit to stand trial on the grounds of insanity, or 3. lack of criminal responsibility has been proven or cannot be ruled out (section 3 of the Youth Courts Act) and the corresponding entry in the Federal Central Criminal Register or the Youth Register has not yet expired or been deleted." (Section 81g [DNA Analysis]). In addition, the person must be suspected of a criminal offence "*of substantial significance or of a crime against sexual self-determination*" or be a person who "*habitually commits other criminal offences*" (Section 81g (1)).

Belgium's law states: "*Art. 5b. 1 § 1. If, after consulting the national unit, it appears that the DNA profile of the convicted or detained has not yet been established, the public prosecutor may order, if necessary under duress, taking a reference sample on that person*".[207] The individual must be being investigated (or be convicted) for one of a list of serious offences (Article 5).

The Netherlands' Code of Criminal Procedure states[208]: "*Section 151b*
1. The public prosecutor may order in the interest of the investigation for the purpose of DNA testing as referred to in section 151a(1) that cellular material be taken from the suspect of a serious offence as defined in section 67(1), against whom there are serious suspicions, if he refuses to give his written consent. Section 151a(2) and (4) to (10) inclusive shall apply mutatis mutandis.

2. The public prosecutor shall not issue the order until after the suspect has been given the opportunity to be heard. The suspect may have the legal representation of a defence counsel when he is heard".

In Australia, the state of Victoria's Victoria Crimes Act 1958 states[209]:
"*464T Court may order compulsory procedure*
If— a person refuses to undergo a forensic procedure after being requested to do so or is incapable of giving informed consent by reason of mental impairment; and the sample or examination sought may be obtained by a compulsory procedure; and the person is a relevant suspect; and a member of the police force believes on reasonable grounds that the person has committed the offence in respect of which the procedure was requested— the member may apply to the Magistrates' Court for an order directing the person to undergo the compulsory procedure.
An application under subsection (1) — must be in writing supported by evidence on oath or by affidavit; and if the person is a detained or protected person, must state that fact and identify the place where the person is held or resides; and must specify the type of compulsory procedure sought to be conducted.
The Court may make an order directing a person to undergo a compulsory procedure if the Court is satisfied on the balance of probabilities that—the person is a relevant suspect; and
there are reasonable grounds to believe that the person has committed the offence in respect of which the application is made; and (c) in the case of an application for a sample other than one referred to in paragraph (d), any of the following applies—material reasonably believed to be from the body of a person who committed the offence has been found—at the scene of the offence; or on the victim of the offence or on anything reasonably believed to have been worn or carried by the victim when the offence was committed; or on an object or person reasonably believed to have been associated with the commission of the offence; or (ii) there are reasonable grounds to believe that, because of the nature of the offence or injuries inflicted during the commission of the offence, material from the body or clothing of the victim is present— on the person who committed the offence or on anything reasonably believed to have been worn or carried by that person when the offence was committed; or on an object reasonably believed to have been associated with the commission of the offence; or (iii) the victim of the offence has not been found, and there are reasonable grounds to believe that material reasonably believed to be from the body of the victim is present on a person suspected of having committed the offence; or (iv) the offence in respect of which the application is made is an offence against a provision of Subdivision (8A), (8B) or (8C) of Division 1 of Part I and there are reasonable grounds to believe that the conduct of the procedure on the person may be relevant in determining the paternity of a child that has been conceived allegedly as a result of the offence; and in the case of an application to take a sample or washing from the skin to determine the presence of gunshot residue, a firearm was discharged during the commission of the offence; and in the case of an application to conduct a physical examination, the person who committed the offence had distinguishing marks or injuries, whether acquired during the commission of the offence or otherwise; and there are reasonable grounds to believe that the conduct of the procedure on the person may tend to confirm or disprove his or her involvement in the commission of the offence; and the person has refused to give consent to a request under section 464R(1) or the person is incapable of giving informed consent by reason of mental impairment; and
Except on an application made in accordance with section 464V or 464W, the Magistrates' Court must not make an order directing a person to undergo a compulsory procedure unless the person is present.
A relevant suspect in respect of whom an application is made— is not a party to the application; and may not call or cross-examine any witnesses; and may not address the Court, other than in respect of any matter referred to in subsection (3)(a) to (h).
In exercising the right of address under subsection (5)(c), a relevant suspect may be represented by a legal practitioner.

If the Magistrates' Court makes an order under subsection (3), it must— give reasons for its decision; and state the evidence on which it is satisfied of the matters referred to in subsection (3); and cause a note of the reasons to be entered in the records of the Court; and inform the person ordered to undergo a compulsory procedure that a member of the police force may use reasonable force to enable the procedure to be conducted.
(8) A failure of the Court to comply with subsection (7) does not invalidate any order made by it but constitutes non-compliance for the purposes of section 464ZE(1)(a).
(9) If— a member of the police force proposes to make an application to the Magistrates' Court under subsection (1) in respect of a person; and the person is a detained or protected person— the Court may, on the application of a member of the police force, issue a warrant directing the officer-in-charge of the place where the person is held to deliver the person into the custody of the applicant or another member of the police force for the purpose— of attending the hearing of the application under subsection (1); and if that application is granted, of conducting the procedure on the person.
(10) A member of the police force into whose custody the person is delivered under a warrant issued under subsection (9) must return the person to the officer-in-charge of the place where the person was held— forthwith after the hearing of the application under subsection (1); or if the application is granted, within such period after the hearing of the application as reasonably permits the conduct of the procedure on the person."

A number of other countries restrict their DNA database to convicted persons only. For example, Russia restricted its DNA database to convicted prisoners in legislation adopted in December 2008. Mandatory registration on the DNA database applies to:
"*1) persons convicted and serving a sentence of imprisonment for committing grave or especially grave crimes, as well as all categories of crimes against sexual inviolability and sexual freedom of the individual;*
2) unidentified persons, the biological material which is removed during the production of the investigation." Federal Law of the Russian Federation dated December 3, 2008 N 242-FZ 'On State Genomic Registration in the Russian Federation'.[210]

Annex C: Examples of Provisions for the Destruction of Biological Samples

The German Code of Criminal Procedure[211] states:
"*(2) The cell tissue collected may be used only for the molecular and genetic examination referred to in subsection (1); it shall be destroyed without delay once it is no longer required for that purpose. Information other than that required in order to establish the DNA profile or the gender may not be ascertained during the examination; tests to establish such information shall be inadmissible*".
(Section 81g(2)).

Malaysia adopted DNA legislation in 2009 and detailed regulations in 2012.[212,213] The law states:
"*Storage and disposal of intimate and non-intimate samples*
16. (1) The Head of DNA Databank shall safely and securely store all intimate samples and non-intimate samples that are collected for the purpose of forensic DNA analysis, the portions of the samples that the Head of DNA Databank consider appropriate and without delay destroy any remaining portions.
(2) The procedures for the storage and disposal of an intimate sample and a non-intimate sample shall be as prescribed."
The regulations reiterate:
"*Disposal of intimate and non-intimate sample*
15.(1) The Head of the DNA Databank shall, without delay, destroy any remaining portion of intimate or non-intimate sample according to the standard laboratory procedure".

In South Africa, the law states, in Article 15Q[214]:
"*(5) Any bodily sample taken from a person from the commencement of this Chapter and which is not a crime scene sample must be destroyed and disposed of within three months after a forensic DNA profile is obtained and loaded on the NFDD.*
(6) Records of the destruction of bodily samples must be kept by the authorised officer in the prescribed manner and must be reported to the Board annually".

The Republic of Korea's DNA legislation states[215]:
"*Article 12 (Destruction of DNA Samples)*
(1) When the person in charge of DNA identification information completes storing DNA identification information in the database, he/she shall destroy DNA samples collected pursuant to Article 5 or 6 and DNA extracted from such samples without delay.
(2) Necessary matters concerning the method of, and procedure for, destruction of DNA samples and DNA extracted therefrom shall be prescribed by Presidential Decree."

Tanzania's DNA law states[216]:
"*58.-(1) After disclosure of genetic information to the requesting authority, the samples for Human DNA, processed genetic material and genetic information shall be destroyed in the following manner:*

- *(a) for paternity and civil matters, it shall be six months after the date of disclosure, unless there is a pending appeal where the sample for Human DNA is at issue;*
- *(b) for criminal matters, the sample for Human DNA and any processed genetic materials shall be destroyed after the extraction of the genetic information;*
- *(c) the sample for Human DNA and any processed genetic materials, within one month after the date of the disclosure;*
- (d) *in case no one has requested the destruction of the sample for Human DNA and processed genetic materials after twelve months from the date of disclosure, the designated laboratory in custody of such sample shall destroy sample for Human DNA and any processed materials*".

New Zealand's law states[217]:
60A (2) "*The Commissioner must ensure that the bodily sample referred to in subsection (1)(a) is destroyed as soon as practicable after a DNA profile is obtained from the sample*".

Annex D: Examples of Expungement Requirements for Data Collected from Innocent Persons

Malaysia adopted DNA legislation in 2009 and detailed regulations in 2012.[218,219] The law states:
"*Removal of DNA profile and information from suspected persons index*
17. Where an intimate sample or a non-intimate sample has been taken in accordance with this Act from a person reasonably suspected of having committed an offence and—
(a) investigations reveal that he was not involved in the commission of any offence;
(b) the charge against him in respect of any offence is withdrawn;
(c) he is discharged by a court of an offence with which he has been charged, at trial or on appeal;
(d) he is acquitted of an offence with which he has been charged, at trial or on appeal; or
(e) he is not charged in any court for any offence within a period of one year from the date of taking of such sample from him, the Head of DNA Databank shall, within six months of so being notified by the Officer in Charge of a Police District of the fact referred to in paragraph (a), (b), (c), (d), or (e), remove the DNA profile and any information in relation thereto of such person from the DNA Databank."
The regulation adds:
"*Removal of the DNA profile and information from suspected person's index*
16.(1) Subject to section 17 of the Act, the Officer in Charge of a Police District shall notify the Head of the DNA Databank for removal of the DNA profile and any information in relation thereto from suspected person's index in the form specified in the Fourth Schedule.
(2) The suspected person shall be informed in writing to his last known address that his DNA profile and any information in relation thereto has been removed from the DNA Databank".

The Republic of Korea's DNA legislation states:[220]
"*Article 13 (Erasure of DNA Identification Information)*
(1) If a judgment for acquittal, exoneration, or dismissal of public prosecution or a decision of dismissal of public prosecution is finally and conclusively affirmed for a prisoner in a retrial, the person in charge of DNA identification information shall, ex officio or at the prisoner's request, erase DNA identification information collected pursuant to Article 5 and stored in the database.
(2) If any of the following events occurs to a detained suspect, the person in charge of DNA identification information shall, ex officio or at the suspect's request, erase DNA identification information collected pursuant to Article 6 and stored in the database:
1. If the public prosecutor makes a disposition of "cleared of suspicion" "not guilty" or "not prosecutable" or if the designation of the crime that the detained suspect allegedly perpetrated is changed from the designation of a crime under any subparagraph of Article 5 (1) to the designation of a crime not specified in any subparagraph of the aforesaid paragraph in the course of investigation or trial: Provided, That cases where the public prosecutor makes an independent demand for a disposition of medical treatment and custody pursuant to subparagraph 1 of Article 7 of the Medical Treatment and Custody Act, along with a disposition of "not guilty" shall be excluded herefrom;
2. If a judgment of acquittal, exoneration, or dismissal of public prosecution by a court or a decision of dismissal of public prosecution is finally and conclusively affirmed: Provided, that cases where a sentence of medical treatment and custody is imposed along with a judgment of acquittal shall be excluded herefrom;
3. If a judgment by a court of dismissal of an independent demand for a disposition of medical treatment and custody under subparagraph 1 of Article 7 of the Medical Treatment and Custody Act is finally and conclusively affirmed.
(3) If a prisoner or a detained suspect is dead, the person in charge of DNA identification information shall, ex officio or at the request of any of the deceased's relatives, erase DNA identification information collected pursuant to Article 5 or 6 and stored in the database:

(4) If it is no longer necessary to preserve and manage DNA identification information collected pursuant to Article 7 and stored in the database because the identify has been ascertained or due to any other reason, the person in charge of DNA identification information shall, ex officio or at the identified person's request, erase the DNA identification information.
(5) When the person in charge of DNA identification information erases DNA identification information pursuant to any provision of paragraphs (1) through (4), he/she shall notify the relevant person or the requesting person of the erasure within 30 days.
(6) Necessary matters concerning the method of, and procedure for, erasing DNA identification information and notification shall be prescribed by Presidential Decree."

Germany's law on the data of DNA analysis states[221]: "*8.4 The data shall be erased if their storage is inadmissible or no longer necessary ($ 32 para. 2, 9 sentence 1 BKAG).*
• Storage is not permitted if the accused is acquitted, the commencement of the trial against him/her has been incontestably rejected, or the procedure has not been set only provisionally and it can be seen from the decision grounds that the person concerned has not committed to act unlawfully ($ 8 Abs . 3 BKAG).
• the data of an accused are also deleted when no longer any reason to believe that criminal proceedings against him/her shall be maintained for offences with considerable importance ($ 8 para. 1 no. 1 in conjunction BKAG $ 3 sentence 3 DNA Identity Act)".

South Africa's DNA law contains the following provisions for deletion of DNA profiles:
"*Arrestee Index*
15I. (1) The Arrestee Index must contain forensic DNA profiles, derived by means of forensic DNA analysis, from a bodily sample taken under any power conferred by Chapter 3 of the Criminal Procedure Act where an arrestee's forensic DNA profile does not form part of any other Index.
(2) The forensic DNA profile in the Arrestee Index must be removed by the authorised officer immediately upon application, in the prescribed manner, when a—
(a) child is diverted in accordance with Chapter 8 of the Child Justice Act, 2008 (Act No. 75 of 2008);
(b) decision was made not to prosecute a person;
(c) person is discharged at a preparatory examination; or
(d) person is acquitted at his or her trial:
Provided that there is no other outstanding criminal investigation against the person.
(3) The application referred to in subsection (2) must be submitted to the authorised officer and a copy thereof provided to the Board.
(4) If no application for removal of a forensic DNA profile, contemplated in subsection (2) is received, the profile of the relevant person must be removed immediately after the authorised officer has been notified in accordance with subsection (5) or (6), but may not be retained for longer than—
(a) three years, in the case of an adult; or
(b) twelve months, in the case of a child.
(5) The Clerk of the Court or Registrar of the High Court must notify the authorised officer of an acquittal, conviction, setting aside or finding of a preliminary investigation within 60 days from the date of the verdict or outcome of the matter.
(6) In respect of a decision not to prosecute or the diversion of a child in accordance with Chapter 8 of the Child Justice Act, the prosecutor who made the decision must notify the authorised officer within 60 days from the date of the decision.
(7) If an application contemplated in subsection (2) is received by the authorised officer before a notification referred to in subsection (5) or (6) has been received, the authorised officer must enquire from the relevant authority in that regard.
(8) The authorised officer must notify the relevant person referred to in subsection (2) of the removal of his or her forensic DNA profile from the Arrestee Index.

(9) The authorised officer must inform the Board quarterly of any removal of a forensic DNA profile from the Arrestee Index in terms of subsections (2) and (4)".

New Zealand's law states[222]:
"*24P Information that may be kept on Part 2B temporary databank*
A DNA profile derived from a bodily sample taken under this Part may be stored on a Part 2B temporary databank only if—
(a) the person from whom the bodily sample was taken has been charged with the triggering offence, or a related relevant offence; and
(b) circumstances have not yet arisen where—
(i) records of the DNA profile must be destroyed under section 60A; or
(ii) the DNA profile may be stored on a DNA profile databank under section 26(ab) or (ac).
24Q Removal of DNA profiles from Part 2B temporary databank
When either of the circumstances in section 24P(b)(i) or (ii) has arisen in relation to a DNA profile, the DNA profile must be removed from the Part 2B temporary databank".
Section 60A is given as:
"*20 New section 60A inserted*
The following section is inserted after section 60:
60A Disposal of bodily samples and identifying information obtained under Part 2B
(1) This section applies to—
(a) a bodily sample taken under Part 2B; and
(b) every record of any analysis of that bodily sample carried out on behalf of any constable; and
(c) every record, to the extent that it contains—
(i) information about the sample; and
(ii) particulars that are identifiable by any person as particulars identifying that information with the person from whom the sample was taken.
(2) The Commissioner must ensure that the bodily sample referred to in subsection (1)(a) is destroyed as soon as practicable after a DNA profile is obtained from the sample.
(3) The Commissioner must ensure that any record referred to in subsection (1)(b) and (c) is destroyed,—
(a) subject to section 61, as soon as practicable after the expiry of the period of 2 months beginning on the date on which the sample is taken, if the person is not charged with the triggering offence, or a related relevant offence, before the expiry of that period; or (b) if the person is charged with such an offence before the expiry of that period, as soon as practicable after the first of the following to occur:
(i) the charge is withdrawn; or
(ii) the person is acquitted of the offence.
(4) Nothing in this section requires the destruction of a DNA profile that may lawfully be retained in a DNA profile databank.
21 Extension of period for which sample may be retained
(1) Section 61 is amended by repealing subsection (1) and substituting the following subsections:
(1) On application in accordance with this section, a High Court Judge may,—
"(a) in respect of a bodily sample taken under Part 2 and related records as described in section 60(1)(b) and (c), extend the period specified in section 60(1)(d); or
(b) in respect of records as described in section 60A(1)(b) and (c), extend the period specified in section 60A(3)(a).
(1A) In this section, the period in section 60(1)(d) or, as the case may be, section 60A(3)(a) is referred to as the relevant period."
Section 61 is also amended by repealing subsection (3) and substituting the following subsections:
"*(3) An extension or, as the case requires, a further extension of the relevant period may be granted under this section only if the High Court Judge is satisfied—*

(a) that the person from whom the bodily sample was taken has not been charged with the triggering offence, or a related relevant offence; and
(b) either of the circumstances mentioned in subsection (3A) exists.
(3A) The circumstances referred to in subsection (3) are—
(a) that there is still good cause to suspect that the person committed an offence referred to in subsection (3)(a) and—
(i) there is a good reason for the person not having been charged; and
(ii) it is important to the investigation of the offence that the bodily sample, and any records that would otherwise be required to be destroyed, be retained; or
(b) that—
(i) there is not, or no longer, good cause to suspect that the person committed an offence referred to in subsection (3)(a); but
(ii) it is important to the investigation of the offence, or to criminal proceedings in relation to that offence, that the bodily sample, and any records that would otherwise be required to be destroyed, be retained."

The US state of Maryland requires[223]:
"*§ 2-511. Expungement of DNA information [Amendment subject to abrogation].*
(a) Conditions; exception.-
(1) Except as provided in paragraph (2) of this subsection, any DNA samples and records generated as part of a criminal investigation or prosecution shall be destroyed or expunged automatically from the State DNA data base if:
(i) a criminal action begun against the individual relating to the crime does not result in a conviction of the individual;
(ii) the conviction is finally reversed or vacated and no new trial is permitted; or
(iii) the individual is granted an unconditional pardon.
(2) A DNA sample or DNA record may not be destroyed or expunged automatically from the State DNA data base if the criminal action is put on the stet docket or the individual receives probation before judgment.
(b) Case in which eligibility for expungement was established.- If the DNA sample or DNA record was obtained or generated only in connection with a case in which eligibility for expungement has been established, the DNA sample shall be destroyed and the DNA record shall be expunged.
(c) Expungement from all local, State, and federal data bases.- Any DNA record expunged in accordance with this section shall be expunged from every data base into which it has been entered, including local, State, and federal data bases.
(d) Period for expungement or destruction.- An expungement or destruction of sample under this section shall occur within 60 days of an event listed in subsection (a) of this section.
(e) Documenting letter.- A letter documenting expungement of the DNA record and destruction of the DNA sample shall be sent by the Director to the defendant and the defendant's attorney at the address specified by the court in the order of expungement.
(f) Use or admissiblity of qualifying record or sample.- A record or sample that qualifies for expungement or destruction under this section and is matched concurrent with or subsequent to the date of qualification for expungement:
(1) may not be utilized for a determination of probable cause regardless of whether it is expunged or destroyed timely; and
(2) is not admissible in any proceeding for any purpose.
(g) Procedures.- The Director shall adopt procedures to comply with this section".

The US state of North Carolina's legislation states in § 15A-266.3A[224]:

"(h) The Crime Laboratory shall remove a person's DNA record, and destroy any DNA biological samples that may have been retained, from the State DNA Database and DNA Databank if both of the following are determined pursuant to subsection (i) of this section:

(1) As to the charge, or all charges, resulting from the arrest upon which a DNA sample is required under this section, a court or the district attorney has taken action resulting in any one of the following:

a. The charge has been dismissed.

b. The person has been acquitted of the charge.

c. The defendant is convicted of a lesser-included misdemeanor offense that is not an offense included in subsection (f) or (g) of this section.

d. No charge was filed within the statute of limitations, if any.

e. No conviction has occurred, at least three years has passed since the date of arrest, and no active prosecution is occurring.

(2) The person's DNA record is not required to be in the State DNA Database under some other provision of law, or is not required to be in the State DNA Database based upon an offense from a different transaction or occurrence from the one which was the basis for the person's arrest.

(i) Prior to June 1, 2012, upon the occurrence of one of the events in sub-subdivision d. or e. of subdivision (1) of subsection (h) of this section, the defendant or the defendant's counsel shall provide the prosecuting district attorney with a signed request form, promulgated by the Administrative Office of the Courts, requesting that the defendant's DNA record be expunged from the DNA Database and that any biological samples in the DNA Databank be destroyed. On or after June 1, 2012, upon the occurrence of one of the events in sub-subdivision d. or e. of subdivision (1) of subsection (h) of this section, no request form shall be required and the prosecuting district attorney shall initiate the procedure provided in subsection (j) of this section.

(j) Prior to June 1, 2012, within 30 days of the receipt of the form required by subsection (i) of this section or the occurrence of one of the events in sub-subdivision a., b., or c. of subdivision (1) of subsection (h) of this section; and on or after June 1, 2012, within 30 days of the occurrence of one of the events in subdivision (1) of subsection (h) of this section, the prosecuting district attorney shall determine if a DNA sample was taken pursuant to this section, and if so, shall:

(1) Verify and indicate the facts of the qualifying event on a verification form promulgated by the Administrative Office of the Courts.

(2) Include the last known address of the defendant, as reflected in the court files, on the verification form.

(3) Sign the verification form or, if the defendant was acquitted or the charges were dismissed by the court, obtain the signature of a judge.

(4) Transmit the verification form to the Crime Laboratory.

(k) Within 90 days of receipt of the verification form, the Crime Laboratory shall:

(1) Determine whether the requirement of subdivision (2) of subsection (h) of this section has been met.

(2) If the requirement has been met, remove the defendant's DNA record and samples as required by subsection (h) of this section.

(3) Mail to the defendant, at the address specified in the verification form, a notice doing either of the following:

a. Documenting expunction of the DNA record and destruction of the DNA sample.

b. Notifying the defendant that the DNA record and sample do not qualify for expunction pursuant to subsection (h) of this section.

(l) The defendant may file a motion with the court to review the denial of the defendant's request or the failure of either the district attorney or the Crime Laboratory to act within the prescribed time period.

(m) Any identification, warrant, probable cause to arrest, or arrest based upon a database match of the defendant's DNA sample which occurs after the expiration of the statutory periods prescribed for

expunction of the defendant's DNA sample, shall be invalid and inadmissable in the prosecution of the defendant for any criminal offense.
(n) Notwithstanding subsection (h) of this section, the Crime Laboratory is not required to destroy or remove an item of physical evidence obtained from a sample if evidence relating to another person would thereby be destroyed.
(o) The Crime Laboratory shall adopt procedures to comply with this section".

The US state of Tennessee provides that[225]:
"*(e)(2) The clerk of the court in which the charges against a person described in subdivision (e)(1) are disposed of shall notify the Tennessee bureau of investigation of final disposition of the criminal proceedings. If the charge for which the sample was taken is dismissed or the defendant is acquitted at trial, then the bureau shall destroy the sample and all records of the sample; provided, that there is no other pending qualifying warrant or capias for an arrest or felony conviction that would otherwise require that the sample remain in the data bank*".

The US state of Missouri requires[226]:
"*11. When a DNA sample is taken of an arrestee for any offense listed under subsection 1 of this section and charges are filed:*
(1) If the charges are later withdrawn, the prosecutor shall notify the state highway patrol crime laboratory that such charges have been withdrawn;
(2) If the case is dismissed, the court shall notify the state highway patrol crime laboratory of such dismissal;
(3) If the court finds at the preliminary hearing that there is no probable cause that the defendant committed the offense, the court shall notify the state highway patrol crime laboratory of such finding;
(4) If the defendant is found not guilty, the court shall notify the state highway patrol crime laboratory of such verdict.
If the state highway patrol crime laboratory receives notice under this subsection, such crime laboratory shall determine, within thirty days, whether the individual has any other qualifying offenses or arrests that would require a DNA sample to be taken. If the individual has no other qualifying arrests or offenses, the crime laboratory shall expunge all DNA records in the database pertaining to such person and destroy the person's DNA sample".

US Federal law requires the expungement of records only when notification is received of the relevant court orders.[227] This procedure is adequate only when state law requires the notifications to be sent automatically to the relevant agencies (as in some of the state provisions sited above):
"*(d) Expungement of records*
(1) By Director
(A) The Director of the Federal Bureau of Investigation shall promptly expunge from the index described in subsection (a) of this section the DNA analysis of a person included in the index—
(i) on the basis of conviction for a qualifying Federal offense or a qualifying District of Columbia offense (as determined under sections 14135a and 14135b of this title, respectively), if the Director receives, for each conviction of the person of a qualifying offense, a certified copy of a final court order establishing that such conviction has been overturned; or
(ii) on the basis of an arrest under the authority of the United States, if the Attorney General receives, for each charge against the person on the basis of which the analysis was or could have been included in the index, a certified copy of a final court order establishing that such charge has been dismissed or has resulted in an acquittal or that no charge was filed within the applicable time period.
(B) For purposes of subparagraph (A), the term "qualifying offense" means any of the following offenses:

(i) A qualifying Federal offense, as determined under section 14135a of this title.
(ii) A qualifying District of Columbia offense, as determined under section 14135b of this title.
(iii) A qualifying military offense, as determined under section 1565 of title 10.
(C) For purposes of subparagraph (A), a court order is not "final" if time remains for an appeal or application for discretionary review with respect to the order.
(2) By States
(A) As a condition of access to the index described in subsection (a) of this section, a State shall promptly expunge from that index the DNA analysis of a person included in the index by that State if—
(i) the responsible agency or official of that State receives, for each conviction of the person of an offense on the basis of which that analysis was or could have been included in the index, a certified copy of a final court order establishing that such conviction has been overturned; or
(ii) the person has not been convicted of an offense on the basis of which that analysis was or could have been included in the index, and the responsible agency or official of that State receives, for each charge against the person on the basis of which the analysis was or could have been included in the index, a certified copy of a final court order establishing that such charge has been dismissed or has resulted in an acquittal or that no charge was filed within the applicable time period.
(B) For purposes of subparagraph (A), a court order is not "final" if time remains for an appeal or application for discretionary review with respect to the order".

Annex E: Limits on Retention of DNA Profiles from Persons Convicted of Minor Crimes

Germany's law on the data of DNA analysis states[228]: "*8.1 The entries shall be examined in the context of the individual case management and*
• for accused adults after ten years
• for accused youths after five years
whether to correct or delete the data ($ 32 para 3 BKAG;. $ 32 para 9 BKAG for the obligations of the regions). Sentence 1 shall apply accordingly to convicted /equivalent persons.
8.2 The period begins on the date on which the last event occurred, which led to the storage of the data, but not before the release of the person concerned from a correctional facility or before the removal of a measure of deprivation of liberty for correction and prevention (S 32 para. 5 sentence 1 BKAG)."

New Zealand's law states[229]:
"*9 New sections 26A and 26B inserted*
The following sections are inserted after section 26:
26A Removal of certain DNA profiles from DNA profile databank
(1) A DNA profile stored on a DNA profile databank must be removed from the databank and destroyed before the expiry of all fixed periods (retention periods) specified in subsection (4) that apply to the storage of the profile.
(2) In the case of a person's DNA profile stored under section 26(a) or (ab), the storage of the profile is subject to subsection (4) if—
(a) the person was a young person on the date of the offence; and
(b) any of the following applies:
(i) a Youth Court made an order under 1 or more of paragraphs (a) to (n) of section 283 of the Children, Young Persons, and Their Families Act 1989; or
(ii) a Youth Court made an order under section 283(o) of the Children, Young Persons, and Their Families Act 1989 but no court imposed a sentence of imprisonment for the offence; or
"(iii) a District Court (rather than a Youth Court) convicted the person of the offence but did not impose a sentence of imprisonment.
(3) In the case of a profile stored under section 26(ac), the storage of the profile is subject to subsection (4) if—
(a) the person was a young person on the date of the offence; and
(b) a Youth Court made an order under section 282 of the Children, Young Persons, and Their Families Act 1989 discharging the information relating to the offence after finding that the offence was proved.
(4) The retention periods and effect of certain subsequent offences are as follows: [specific retention periods are given]
(5) A person's DNA profile stored under section 26 may, unless otherwise provided by this Act, be stored indefinitely on a DNA profile databank if any of the following apply:
(a) if the profile is stored in relation to an offence and a court imposes a sentence of imprisonment for the offence:
(b) if the profile is stored in relation to an offence and a retention period initially applies to the offence and, during that period, a subsequent order or conviction is made or entered against the person that is not specifically provided for in the third column of the table in subsection (4) [examples given]:
(c) in any other case (whether the person is a young person or of or over the age of 17 years), no fixed retention period is specified by this Act".

Brazil's law states[230]:

"*Art 7a. The exclusion of genetic profiles of the databases will occur at the end of the period established by law for the prescription of the offense*. "

Annex F: Examples of Provisions for the Deletion of Data on Request

In addition to its automatic expungement procedure, New Zealand's law states[231]:
"*26B Certain young persons may apply for removal of DNA profiles from DNA profile databank*
(1) This section applies to a person if,—
(a) before the commencement of this section,—
(i) a DNA profile of the person was taken and stored on a DNA databank under Part 2 when the person was a young person; and
(ii) a Youth Court made an order in relation to the person under section 282 or 283 of the Children, Young Persons, and Their Families Act 1989 in relation to an offence but no court imposed a sentence of imprisonment for the offence; and
(b) within 10 years after the date of that order, the person is not convicted of an imprisonable offence.
(2) The person's DNA profile must be removed from the DNA databank and destroyed if the person applies in writing to the Commissioner requesting the removal of the profile."

In addition to its automatic expungement procedure, the US state of Missouri's law states[232]:
"*9. An individual may request expungement of his or her DNA sample and DNA profile through the court issuing the reversal or dismissal. A certified copy of the court order establishing that such conviction has been reversed or guilty plea has been set aside shall be sent to the Missouri state highway patrol crime laboratory. Upon receipt of the court order, the laboratory will determine that the requesting individual has no other qualifying offense as a result of any separate plea or conviction and no other qualifying arrest prior to expungement.*
(1) A person whose DNA record or DNA profile has been included in the state DNA database in accordance with this section and sections 650.050, 650.052, and 650.100 may request expungement on the grounds that the conviction has been reversed, or the guilty plea on which the authority for including that person's DNA record or DNA profile was based has been set aside.
(2) Upon receipt of a written request for expungement, a certified copy of the final court order reversing the conviction or setting aside the plea and any other information necessary to ascertain the validity of the request, the Missouri state highway patrol crime laboratory shall expunge all DNA records and identifiable information in the state DNA database pertaining to the person and destroy the DNA sample of the person, unless the Missouri state highway patrol determines that the person is otherwise obligated to submit a DNA sample. Within thirty days after the receipt of the court order, the Missouri state highway patrol shall notify the individual that it has expunged his or her DNA sample and DNA profile, or the basis for its determination that the person is otherwise obligated to submit a DNA sample".

Annex G: Example Provisions for the Collection of Samples

Most laws make a distinction between "non-intimate" samples such as mouth swabs which may be taken in police custody and "intimate" samples (e.g. from genitalia following an alleged sexual assault) which require consent and the involvement of a medical professional.
In Ireland, Article 2 states[233]:
"*"intimate sample" means any of the following taken, or to be taken, from a person under section 12:*
(a) a sample of—
(i) blood,
(ii) pubic hair, or
(iii) urine;
(b) a swab from a genital region or a body orifice other than the mouth; or
(c) a dental impression".[234]
And: "*"non-intimate sample" means any of the following taken, or to be taken, from a person under section 13:*
(a) a sample of—
(i) saliva,
(ii) hair other than pubic hair,
(iii) a nail, or
(iv) any material found under a nail;
(b) a swab from any part of the body including the mouth but not from any other body orifice or a genital region; or
(c) a skin impression".
Section 13 describes the rules for the taking of "non-intimate" samples, where consent is not required for certain categories of suspects. More details are given in section 12 for the taking of intimate samples, which require the consent of the individual:
"*Taking of intimate samples from persons in custody of Garda Síochána*
12. (1) Subject to this Act, a member of the Garda Síochána may take, or cause to be taken, an intimate sample under this section from a person who is detained under any of the provisions referred to in section 9(1) for the purposes of forensic testing and, if appropriate, the generation of a DNA profile in respect of the person to be entered in the reference index of the DNA Database System.
(2) An intimate sample may be taken under this section only if—
(a) a member of the Garda Síochána not below the rank of inspector authorises it to be taken for the purposes specified in subsection (1), and
(b) the appropriate consent has been given in writing to the taking of the sample.
(3) An authorisation to take an intimate sample under this section shall not be given unless the member of the Garda Síochána giving it has reasonable grounds—
(a) for suspecting the involvement of the person from whom the sample is to be taken in the commission of the offence in respect of which he or she is detained, and
(b) for believing that the sample will tend to confirm or disprove the involvement of that person in the commission of the offence concerned.
(4) The results of the forensic testing of an intimate sample may be given in evidence in any proceedings.
(5) Before a member of the Garda Síochána seeks the consent of a person from whom an intimate sample is required to the taking of such a sample or the member takes, or causes to be taken, such a sample from the person, the member shall inform the person of the following:

(a) the nature of the offence in the commission of which it is suspected that the person has been involved;
(b) that an authorisation to take the sample from him or her has been given under subsection (2)(a) and the grounds on which it has been given;
(c) that in a case in which an intimate sample already taken from the person has proved to be insufficient—
(i) that that sample has proved to be insufficient, and
(ii) that either—
(I) another authorisation under subsection (2)(a) is not, by virtue of section 3(6), required, or
(II) an authorisation to take a second intimate sample from him or her has, in accordance with section 25(1), been given under subsection (2)(a) and the grounds on which it has been given;
(d) that the results of the forensic testing of the sample may be given in evidence in any proceedings;
(e) if appropriate, the matters referred to in subsections (2) and (3) of section 19 if that section is to have effect in relation to the person;
(f) if appropriate, that the sample will be used to generate a DNA profile in respect of the person to be entered in the reference index of the DNA Database System and the effect of such an entry;
(g) that the sample, or the DNA profile generated from the sample in respect of the person, may be transmitted or provided to a person or body in connection with the investigation of criminal offences or criminal proceedings (whether within or outside the State) as provided for in or permitted by this Act;
(h) that the sample may be compared under section 145 with evidence taken from a crime scene (including crime scene samples) received from a law enforcement agency within the meaning of Chapter 7 of Part 12; and
(i) that the sample may be destroyed, and (if appropriate) the DNA profile in respect of the person entered in the reference index of the DNA Database System may be removed from that System, in accordance with Part 10.
(6) If a person expressly withdraws the appropriate consent given under subsection (2)(b) (or if the withdrawal of that consent can reasonably be inferred from the conduct of the person) before or during the taking of an intimate sample under this section—
(a) that withdrawal of consent shall be treated as a refusal to give the appropriate consent to the taking of the sample under this section, and
(b) the provisions of this Part shall apply accordingly.
(7) A withdrawal under subsection (6) of the appropriate consent given under subsection (2)(b) shall be recorded in writing by a member of the Garda Síochána as soon as practicable after such withdrawal.
(8) The appropriate consent given under subsection (2)(b) to the taking of an intimate sample under this section may not be withdrawn after the sample has been taken".
Section 15 describes appropriate consent to taking of intimate samples, Section 16 outlines the procedure for an application for a court order authorising taking of intimate sample from protected person, and Section 16 describes the procedure for an application for a court order authorising taking of intimate sample from child. Section 18 requires the involvement of a medical practitioner or nurse in the collection of intimate samples:
"*Persons authorised to take intimate samples*
18. (1) A sample of blood or pubic hair or a swab from a genital region or a body orifice other than the mouth may be taken under this Part <u>only by a registered medical practitioner or a registered nurse</u>.
(2) A dental impression may be taken under this Part only by a registered dentist or a registered medical practitioner.

(3) An intimate sample other than a sample of blood or a dental impression shall, in so far as practicable, be taken by a person who is of the same sex as the person from whom the sample is being taken under this Part."

The Netherlands' Code of Criminal Procedure states (Section 151b): "3. *The order shall be executed by taking a cheek swab. If, for special medical reasons or on account of the suspect's resistance, taking a cheek swab is undesirable or does not provide suitable cellular material, a blood or hair root sample shall be taken, if necessary with the assistance of the police. The cellular material shall be taken by a medical doctor or a nurse. In cases to be designated by Governmental Decree, the cellular material may be taken by a person who meets requirements to be set by or pursuant to Governmental Decree*".

South Australia Criminal Law (Forensic Procedures) Act 2007 states[235]:
"*Part 3—Carrying out forensic procedures*
Division 1—General provisions on carrying out forensic procedures
21—Forensic procedures to be carried out humanely
(1) A forensic procedure must be carried out humanely and with care—
(a) to avoid, as far as reasonably practicable, offending genuinely held cultural values or religious beliefs; and
(b) to avoid inflicting unnecessary physical harm, humiliation or embarrassment.
(2) A forensic procedure must not be carried out in the presence or view of more persons than are necessary for properly carrying out the procedure and satisfying any relevant statutory requirements.
(3) If reasonably practicable, a forensic procedure that involves exposure of, or contact with, the genital or anal area, the buttocks or, in the case of a female, the breasts must not be carried out by a person of the opposite sex (other than at the request of the person on whom the forensic procedure is to be carried out).
22—Right to be assisted by interpreter
If a person on whom a forensic procedure is to be carried out is not reasonably fluent in English, the person is entitled—
(a) to be assisted by an interpreter; and
(b) if the person so requests—to have an interpreter present during carrying out of the forensic procedure.
23—Duty to observe relevant medical or other professional standards
A forensic procedure must be carried out in a way that is consistent with appropriate medical standards or other relevant professional standards.
24—Who may carry out forensic procedure
(1) A person who carries out a forensic procedure must be—
(a) a medical practitioner; or
(b) a person who is qualified as required by the regulations to carry out forensic procedures of the relevant type.
(2) A person carrying out a forensic procedure may be assisted by a police officer or other person.
25—Right to have witness present
(1) If an intrusive forensic procedure is to be carried out on a person, the person must be allowed a reasonable opportunity to arrange for the attendance, at the person's expense, of a medical practitioner of the person's choice to witness the forensic procedure.
(2) If, in accordance with an authorisation under a Division of Part 2, a forensic procedure is to be carried out on a person who is a protected person within the meaning of that Division, an appropriate representative must be present to witness the forensic procedure.
(3) An appropriate representative may be—
(a) a relative or friend chosen by, or acceptable to, the protected person; or

(b) if there is no available person within the above category—an advocate for the protected person nominated by a government or private agency with responsibilities for the care of protected persons of the relevant class; or

(c) if there is no available person within either of the above categories—a person, who is not a police officer or person involved in the investigation of the suspected offence (if any), chosen by a police officer in charge of a police station or, where relevant, the investigating police officer.

(4) However, a witness who attempts, without reasonable justification, to obstruct the forensic procedure may be excluded from the place in which the procedure is being or is to be carried out.

26—Audiovisual record of intrusive procedures to be made

(1) An audiovisual recording of an intrusive forensic procedure must be made—

(a) if the procedure is a suspects procedure; or

(b) if the procedure is a volunteers and victims procedure and the person on whom the procedure is to be carried out requests the making of an audiovisual record.

(2) Arrangements must be made, at the request of the person on whom the intrusive forensic procedure was carried out, for the playing of the audiovisual recording of the procedure at a reasonable time and place to be nominated by the Commissioner of Police.

(3) A copy of an audiovisual recording made under this section must, on payment of the fee fixed by regulation, be made available to the person on whom the forensic procedure was carried out.

27—Exemption from liability

No civil or criminal liability is incurred by a person who carries out, or assists in carrying out, a forensic procedure for an act or omission if—

(a) the person genuinely believes that the forensic procedure is authorised under this Act; and

(b) the act or omission is reasonable in the circumstances".

Annex H: Examples of Provisions Regarding Vulnerable Persons

In relation to the collection of DNA under warrant, Canadian law states:
"(4) A young person against whom a warrant is executed has, in addition to any other rights arising from his or her detention under the warrant,
(a) the right to a reasonable opportunity to consult with, and
(b) the right to have the warrant executed in the presence of counsel or a parent or, in the absence of a parent, an adult relative or, in the absence of a parent and an adult relative, any other appropriate adult chosen by the young person.
(5) A young person may waive his or her rights under subsection (4) but any such waiver
(a) must be recorded on audio tape or video tape or otherwise; or
(b) must be made in writing and contain a statement signed by the young person that he or she has been informed of the right being waived". [236]

The EU Data Protection Directive[237] states (39): "*In order to enable him or her to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, using clear and plain language. Such information should be adapted to the needs of vulnerable persons such as children*" and (50) "*The measures taken by the controller should include drawing up and implementing specific safeguards in respect of the treatment of personal data of vulnerable persons such as children*".

Ireland has a number of legislative provisions regarding vulnerable persons and children[238], including Article 14:
"*Giving of information under Part 2 to protected persons or children*
14. (1) The information to be given under section 12(5), 13(5), 16(2) or 24(4) shall, in the case of a protected person, be given insofar as it is practicable to do so in a manner and in language that are appropriate to the level of understanding of the person.
(2) The information to be given under section 11(3) (if appropriate), 12(5), 13(5), 17(2) or 24(4) shall, in the case of a child, be given insofar as it is practicable to do so in a manner and in language that are appropriate to the age and level of understanding of the child."
Article 22 covers the taking of samples from children under Part 2; Article 23 covers persons other than parent or guardian to support protected person; Article 32 covers the taking of samples from child offenders; Article 37 covers the giving of information under Part 4 to protected persons or children; Articles 53 to 58 cover the taking of certain samples under Parts 3 and 6 from protected persons or children; and Article 84 covers the removal of DNA profiles in respect of former child offenders from DNA Database.

The New South Wales Crimes (Forensic Procedures) Act 2000 puts in place a special procedure for Aboriginal persons and Torres Strait Islanders[239]:
"*s10. Informed consent to forensic procedures—Aboriginal persons and Torres Strait Islanders*
(1) This section applies where:
(a) a police officer intends to ask a suspect to consent to a forensic procedure, and
(b) the suspect identifies as an Aboriginal person or Torres Strait Islander.
(2) A suspect gives informed consent to a forensic procedure if the suspect consents after a police officer:
(a) asks the suspect to consent to the forensic procedure under section 11, and
(b) gives the suspect a written statement setting out:
(i) the information that the suspect must be given under section 13 (1) (a), (e), (f), (g), (h), (i), (j) and (k), and
(ii) the nature of the information that the suspect must be given under section 13 (1) (b), (c) and (d) (but not the specific information that the suspect is to be given under these paragraphs in relation to

the particular forensic procedure), and
(c) informs the suspect about the forensic procedure in accordance with section 13, and
(d) complies with the rest of this section.
(3) The police officer must not ask the suspect to consent to the forensic procedure unless:
(a) an interview friend is present, or
(b) the suspect has expressly and voluntarily waived his or her right to have an interview friend present.
Note. Section 106 relates to proving a waiver under paragraph (b).
(4) Before asking the suspect to consent to a forensic procedure, the police officer must:
(a) inform the suspect that a representative of an Aboriginal legal aid organisation will be notified that the suspect is to be asked to consent to a forensic procedure, and
(b) notify such a representative accordingly.
(5) The police officer is not required to comply with subsection (4) if he or she is aware that the suspect:
(a) has arranged for a legal representative to be present, or
(b) has expressly and voluntarily waived his or her right to have a legal representative present,
while the suspect is being asked to consent to the forensic procedure.
(6) After asking a suspect covered by subsection (3) (b) to consent to a forensic procedure, the police officer must give the suspect a reasonable opportunity to communicate, or attempt to communicate, with an Australian legal practitioner of the suspect's choice and, subject to subsection (8), to do so in private.
(7) After asking a suspect not covered by subsection (3) (b) to consent to a forensic procedure, the police officer must allow the suspect to communicate with the interview friend (if any), and with the suspect's legal representative (if any), and, subject to subsection (8), to do so in private.
(8) If a suspect covered by subsection (6) or (7) is under arrest, the police officer need not allow the suspect to communicate, or attempt to communicate, with the Australian legal practitioner, or the suspect's interview friend or legal representative, in private if the police officer suspects on reasonable grounds that the suspect might attempt to destroy or contaminate any evidence that might be obtained by carrying out the forensic procedure.
(9) An interview friend (other than a legal representative) of the suspect may be excluded from the presence of the police officer and the suspect if:
(a) the interview friend unreasonably interferes with or obstructs the police officer in asking the suspect to consent to the forensic procedure, or in informing the suspect as required by section 13, or
(b) the police officer forms a belief based on reasonable grounds that the presence of the interview friend could be prejudicial to the investigation of an offence because the interview friend may be a co-offender of the suspect or may be involved in some other way, with the suspect, in the commission of the offence.
(10) If an interview friend is excluded under subsection (9), a suspect may choose another person to act as his or her interview friend. If the suspect does not waive his or her right to have an interview friend present and does not choose another person as an interview friend, the police officer may arrange for any person who may act as an interview friend under section 4 to be present as an interview friend."

Annex I: Examples of Provision of Information for Persons from whom DNA is Taken

The EU Data Protection Directive[240] states (26): "*Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data*". Article 12 covers communication and modalities for exercising the rights of the data subject and Article 13 provides for information to be provided to the data subject.

In Portugal, Article 9 of the DNA database law describes the right to information:[241]
"*Prior to sample collection, the subject has the right to information under paragraph 1 Article 10 of the Personal Data Protection Law, with the necessary adaptations, and should be informed in writing, namely:*
a) that their personal data will be entered a personal data file, with the exception of data for persons referred to in paragraph 1 of Article 8;
b) the nature of the data that is extracted from the sample, i.e. the DNA profile;
c) that the DNA profile is stored in the cases admitted to the this law, as part of a DNA profile file, with the exception of data relating to persons referred to in paragraph 1 of Article 8;
d) the possibility of searching the collected profile against existing DNA profiles in the database with express mention of the possibility of using the data for the purposes of criminal investigation, as applicable;
e) that the collected sample can be stored in a biobank in cases admitted in this law."

Tanzania's DNA law states[242]:
"*30.(1) Where the sample for Human DNA is collected for criminal investigation, the sampling office shall inform the person from whom the sample for Human DNA is to be taken-*

(a) that the authorization by the requesting authority has been obtained;
(b) the reasons for taking the sample for Human DNA;
(c) the procedure to be used to collect; and
(d) *that the genetic information to be extracted from that sample for Human DNA may be used as evidence for or against that person*".

New Zealand's law states[243]:
"*24M Information to be given to person*
If a constable proposes to require a person to give a bodily sample under section 24J or 24K, the constable must—

(a) hand to the person a written notice containing the particulars specified in section 24N; and
(b) inform the person in a manner and in language that the person is likely to understand—
(i) what the triggering offence is; and
(ii) of the effect of sections 24P and 24R; and
(iii) of the effect of sections 48A, 49, 49A, 50A, and 54A; and
(iv) that the sample will be analysed; and
(v) that a DNA profile derived from the sample cannot be used as evidence in criminal proceedings; and
(vi) of the effect of section 26(ab) and (ac); and
(vii) of the effect of section 60A.

24N Form and content of notice

A notice given under section 24M—

(a) must be in the prescribed form; and

(b) must contain the following particulars:

(i) a reference to the triggering offence:

(ii) a statement of the effect of sections 24P and 24R:

(iii) a summary of the provisions of sections 48A, 49, 49A, 50A, and 54A relating to the procedure for taking the sample:

(iv) a summary of the provisions of sections 55, 56, and 56A relating to the procedures for the analysis of the sample and the disclosure of the results of the analysis:

(v) a statement of the effect of section 26(ab) and (ac):

(vi) a reference to the provisions of section 60A relating to the destruction of the sample and of any information derived from any analysis of the sample:

(vii) any other particulars that may be prescribed."

In Canada, the law states[244]:

"*487.07 (1) Before executing a warrant, a peace officer shall inform the person against whom it is to be executed of*

(a) the contents of the warrant;

(b) the nature of the investigative procedure by means of which a bodily substance is to be obtained from that person;

(c) the purpose of obtaining a bodily substance from that person;

(d) the possibility that the results of forensic DNA analysis may be used in evidence;

(e) the authority of the peace officer and person under the direction of any other person under the direction of the peace officer to use as much force as is necessary for the purpose of executing the warrant;

(f) in the case of a young person, the rights of the young person under subsection (4)".

Annex J: Example Provisions for Analysis of Crime Scene Evidence

In South Africa, the law states[245]:
"*15Q. (1) Bodily samples and crime scene samples received at the forensic laboratory must be analysed and loaded on the NFDD within 30 days, unless there is a compelling reason in terms of priorities why such samples cannot be analysed and loaded within that period.*
(2) The authorised officer must report to the Board any compelling reason contemplated in subsection (1) when it occurs.
(3) If a sample is not analysed within the period referred to in subsection
(1) such non-compliance will not have any effect on the investigation or prosecution concerned.
(4) The authorised officer must institute disciplinary action for any failure to analyse and load the samples on the NFDD within the period referred to in subsection (1) without a compelling reason."

Regulations add[246]:
"*(4) A forensic analyst attached to the Forensic Science Laboratory must ensure that forensic DNA profiles are derived from a crime sample, bodily sample and buccal sample within 30 days from the receipt thereof at the Forensic Science Laboratory. The forensic analyst must inform the relevant investigating officer of the result of the analysis. The report of the result must be filed by the investigating officer in the police docket*".

Colorado is one of a number of US states that have passed laws requiring DNA evidence from rapes and sexual assaults to be collected and analysed promptly. Colorado's law includes[247]:
"*24-33.5-113. Forensic medical evidence in sexual assault cases - rules - testing - confidentiality - repeal.*
(1) Rules.
(a) On or before thirty days after the effective date of this section, the executive director shall begin the process of promulgating rules for Forensic medical evidence collected in connection with an alleged sexual assault. Not less than ninety days prior to the promulgation of the rules, the division shall convene a representative group of participants as defined in section 24-4-102 (14.5) to solicit input into the development of the rules. The Representative group must include persons affected by the rules and persons responsible for implementation of the rules. The division may convene as many meetings of the representative group as is necessary.
(b) On or before six months after the effective date of this section, the executive director shall promulgate the rules. The rules must include:
(I) a requirement that forensic evidence must be collected if a victim of an alleged sexual assault requests it to be collected;
(ii) standards for what evidence must be submitted to the Colorado Bureau of Investigation or another accredited crime laboratory;
(iii) time frames for when the evidence must be submitted, analyzed, and compared to DNA databases. The rules on time frames must indicate that, once the backlog described in subsection (4) of this section is resolved, evidence that meets the criteria for mandatory submission must be submitted within twenty-one days after receipt by a law enforcement agency".

Annex K: Example Provisions that Require Laboratory Quality Assurance

In the European Union (EU), Council Framework Decision 2009/905/JHA requires forensic laboratories (for both fingerprints and DNA) to be accredited to ISO standard 17025:[248]
"*Article 1*
Objective 1. The purpose of this Framework Decision is to ensure that the results of laboratory activities carried out by accredited forensic service providers in one Member State are recognised by the authorities responsible for the prevention, detection and investigation of criminal offences as being equally reliable as the results of laboratory activities carried out by forensic service providers accredited to EN ISO/IEC 17025 within any other Member State.
2. This purpose is achieved by ensuring that forensic service providers carrying out laboratory activities are accredited by a national accreditation body as complying with EN ISO/IEC 17025".

The UK has a Forensic Science Regulator which monitors compliance, investigates errors and prepares guidance on issues such as the avoidance of contamination.[249] Some US states have similar arrangements, such as the New York Office of Forensic Services.[250]

US Federal law requires[251]:
"*(b) Information. The index described in subsection (a) of this section shall include only information on DNA identification records and DNA analyses that are—*
(1) based on analyses performed by or on behalf of a criminal justice agency (or the Secretary of Defense in accordance with section 1565 of title 10) in accordance with publicly available standards that satisfy or exceed the guidelines for a quality assurance program for DNA analysis, issued by the Director of the Federal Bureau of Investigation under section 14131 of this title;
(2) prepared by laboratories that—
(A) not later than 2 years after October 30, 2004, have been accredited by a nonprofit professional association of persons actively involved in forensic science that is nationally recognized within the forensic science community; and
(B) undergo external audits, not less than once every 2 years, that demonstrate compliance with standards established by the Director of the Federal Bureau of Investigation".
There are specific provisions for proficiency testing[252]:
"(c) Proficiency testing program
(1) Not later than 1 year after the effective date of this Act,[1] the Director of the National Institute of Justice shall certify to the Committees on the Judiciary of the House and Senate that—
(A) the Institute has entered into a contract with, or made a grant to, an appropriate entity for establishing, or has taken other appropriate action to ensure that there is established, not later than 2 years after September 13, 1994, a blind external proficiency testing program for DNA analyses, which shall be available to public and private laboratories performing forensic DNA analyses;
(B) a blind external proficiency testing program for DNA analyses is already readily available to public and private laboratories performing forensic DNA analyses; or
(C) it is not feasible to have blind external testing for DNA forensic analyses.
(2) As used in this subsection, the term "blind external proficiency test" means a test that is presented to a forensic laboratory through a second agency and appears to the analysts to involve routine evidence.
(3) Notwithstanding any other provision of law, the Attorney General shall make available to the Director of the National Institute of Justice during the first fiscal year in which funds are distributed

under this subtitle up to $250,000 from the funds available under part X of Title I of the Omnibus Crime Control and Safe Streets Act of 1968 [42 U.S.C. 3796kk et seq.] to carry out this subsection".

South Africa's law states:
"*Compliance with Quality Management System*
15.P(1) The authorised officer must develop and recommend standards for quality management, including standards for testing the proficiency of forensic science laboratories and forensic analysts conducting forensic DNA analysis.
(2) The standards referred to in subsection (1) must –
(a) comply with the South African National Accreditation System established under section 3 of the Accreditation for Conformity Assessment, Collaboration and Good Laboratory Practice Act, 2006 (Act No. 19 of 2006), and standards set by the International Organization for Standardization;
(b) specify criteria for quality management and proficiency tests applied to the various types of forensic DNA analysis; and
(c) include a system for grading proficiency testing performance to determine whether a laboratory or forensic analyst is performing acceptably".

In Australia, the Queensland Police Powers and Responsibilities Act 2000 states[253]:
"*488B Commissioner may enter into DNA arrangement*
(1) The commissioner may enter into a contract or other arrangement (each a DNA arrangement) with 1 or both of the following about analysing DNA under section 489—
(a) the chief executive (health);
(b) the chief executive officer, however described, of an accredited laboratory.
(2) In this section—
accredited laboratory means a laboratory accredited as complying with ISO/IEC 17025:2005 by—
(a) the National Association of Testing Authorities, Australia; or
(b) another entity the commissioner is satisfied is appropriately qualified to accredit a laboratory for compliance with ISO/IEC 17025:2005.
ISO/IEC 17025:2005 means the standard titled 'ISO/IEC 17025: 2005—General requirements for the competence of testing and calibration laboratories', published jointly by the International Organisation for Standardisation and the International Electrotechnical Commission."

Annex L: Example Provisions on DNA Profiling Standards

To facilitate cross-border sharing the EU developed the European Standard Set (ESS) of loci (DNA markers). The ESS originally included only seven loci[254], which was increased to twelve in 2009, after forensic scientists had highlighted their concerns about the potential for false matches to occur by chance ("adventitious matches") in cross-border sharing[255]. EU member states were given until the end of November 2011 to implement this Resolution.

In the USA, standards are set by the Scientific Working Group on DNA Analysis Methods (SWGDAM) and its predecessor group, the Technical Working Group on DNA Analysis Methods (TWGDAM).[256] Federal legislation authorizing the Federal Bureau of Investigation (FBI) to establish a National DNA Index System also authorized the creation of the Federal DNA Advisory Board. This same legislation recognized the TWGDAM Guidelines and required that they be followed as the national standards until the FBI Director approved quality assurance standards for forensic DNA analysis. The Federal DNA Advisory Board was responsible for recommending quality assurance standards, and revisions as necessary, to the FBI Director and when their statutory time period expired, they charged SWGDAM with this responsibility.

In Portugal, Article 12(2) of the DNA database law states[257]:
"*DNA markers to incorporate in the file DNA profiles are fixed after consultation with the Commission National Data Protection (NCDP), by joint order members of the Government responsible for the justice and health, in accordance with international standards and scientific knowledge on the matter.*"

Annex M: Example Provisions for Elimination Databases

South Africa's DNA law requires an elimination index to be set up as part of the National Forensic DNA Database (NFDD)[258]:

Elimination Index

15L.

(1) The Elimination Index must contain forensic DNA profiles, derived by means of forensic DNA analysis, from a buccal sample taken from—

(a) a police official, or any other person, who as part of his or her official duties attends or processes a crime scene;

(b) a police official or any other person, who may be handling or processing or examining crime scene samples or bodily samples under this Chapter;

(c) any person directly involved in the servicing or calibration of equipment or in laboratories used in the forensic DNA analysis process;

(d) any person who enters an examination area in a forensic DNAlaboratory, or processes, handles or examines crime scene samples or bodily samples, under this Chapter; and

(e)where possible, any person directly involved in the manufacturing of consumables, equipment, utensils or reagents.

(2) From the commencement of this Chapter, all new recruits to the Service must be required to submit a buccal sample for purposes of forensic DNA profiles derived therefrom to be included in the Elimination Index.

(3) The forensic DNAprofiles in the Elimination Index must be stored on the NFDD and be retained, unless the profile has been migrated to another Index or is no longer required.

(4) A person referred to in subsection (1) may apply, in the prescribed manner, to have his or her profile removed from the Elimination Index when it is no longer required.

(5) Nothing in this section prohibits the forensic DNA profile derived from a sample taken from any person mentioned in subsection (1) or (2) to be subjected to a comparative search for purposes referred to in section 15F".

Ireland's law includes (Part 5)[259]:

"*Definitions (Part 5)*

40. In this Part—

"contamination", in relation to a crime scene sample, means the inadvertent incorporation in the crime scene sample of the DNA of a person to whom this Part applies during—

(a) his or her attendance at the crime scene concerned in the execution of his or her duties,

(b) the conduct of the investigation of an offence or incident that may have involved the commission of an offence, or

(c) the examination or analysis of that sample;

"member of the Garda Síochána" has the meaning it has in section 3 of the Act of 2005.

Taking of samples from Garda Síochána personnel for elimination (Garda Síochána) index

41. (1) A sample taken under this section from a person shall be used to generate a DNA profile in respect of the person to be entered in the elimination (Garda Síochána)index of the DNA Database System for the purpose, in relation to the investigation of offences, of ascertaining whether that person has contaminated a crime scene sample.

(2) A sample shall be taken under this section from the following:

(a) a member of the Garda Síochána, other than a member of the Garda Síochána to whom section 42(2)(a) applies, who is appointed as such a member after the commencement of this section;

(b) a person who is, after the commencement of this section, admitted in accordance with the Act of 2005 to training for membership (including as a reserve member within the meaning of section 3 of that Act) of the Garda Síochána, other than such a person to whom section 42(2)(b) applies.

(3) A sample may be taken under this section from—

(a) a member of the Garda Síochána, other than a member of the Garda Síochána to whom section 42(3)(a) applies, who is such a member upon the commencement of this section, or
(b) a person who is, on the commencement of this section, admitted in accordance with the Act of 2005 to training for membership (including as a reserve member within the meaning of section 3 of that Act) of the Garda Síochána, other than such a person to whom section 42(3)(b) applies, only if he or she consents in writing to having such a sample taken from him or her.
(4) A member of the Garda Síochána or an authorised person shall inform a person to whom this section applies of the following before taking, or causing to be taken, a sample under this section from him or her:
(a) that the sample is to be taken from him or her under this section;
(b) in a case in which a sample already taken under this section from the person has proved to be insufficient or was inadequately labelled or for any other reason mentioned in section 47(1) a second or further sample under this section is required to be taken from him or her—
(i) that the first-mentioned sample has proved to be insufficient, was inadequately labelled or that other reason for requiring a second or further sample under this section to be taken, as may be appropriate, and
(ii) that a second or further sample under this section is, in accordance with section 47(1), to be taken from him or her;
(c) that the sample will be used to generate a DNA profile in respect of the person to be entered in the elimination (Garda Síochána) index of the DNA Database System and the effect of such an entry;
(d) that if the person is, at any time after the taking of the sample, assigned to duties relating to the investigation or technical examination of crime scenes or anything found at or recovered from crime scenes, the DNA profile in respect of the person will be transferred from the elimination (Garda Síochána) index to the elimination (crime scene investigators) index of the DNA Database System;
(e) that, in the case of a person referred to in subsection (2)(b) or (3)(b), if he or she is at any time after the taking of the sample appointed as a member of the Garda Síochána, the DNA profile generated from the sample in respect of the person and entered in the elimination (Garda Síochána) index of the DNA Database System may be retained in that index of that System in accordance with subsection (8); and
(f) that the sample may be destroyed, and the DNA profile in respect of the person entered in the elimination (Garda Síochána) index or elimination (crime scene investigators) index, as the case may be, of the DNA Database System may be removed from that System, in accordance with Part 10.
(5) Subject to this Act, a member of the Garda Síochána or an authorised person may take, or cause to be taken, a sample under this section from a person to whom this section applies.
(6) A sample that was taken before the commencement of this section from a person referred to in subsection (3) for the purpose, in relation to the investigation of offences, of ascertaining whether that person has contaminated a crime scene sample, and any DNA profile that was generated from the sample in respect of the person, shall be regarded as a sample taken from him or her under this section and a DNA profile generated from the sample to be entered in the elimination (Garda Síochána)index of the DNA Database System in respect of him or her only if—
(a) that person consents in writing to the sample and DNA profile concerned being so regarded, and
(b) before the consent referred to in paragraph (a) is obtained, subsection (4) shall,with any necessary modifications, be applied in relation to that person.
(7) If a person from whom a sample is taken, or is regarded under subsection (6) as having been taken, under this section is, at any time after the sample is taken or so regarded as having been taken, assigned to duties relating to the investigation or technical examination of crime scenes or anything found at or recovered from crime scenes, the DNA profile that was generated from the sample in respect of the person shall be transferred from the elimination (Garda Síochána) index to the elimination (crime scene investigators) index of the DNA Database System.
(8) If a person referred to in subsection (2)(b) or (3)(b) is at any time after a sample is taken, or in the case of a person referred to in subsection (3)(b) is regarded under subsection (6) as having been

taken, from him or her under this section appointed as a member of the Garda Síochána, the DNA profile generated from the sample in respect of the person and entered in the elimination (Garda Síochána) index of the DNA Database System may be retained in that index of that System as if it were generated from a sample taken from the person under subsection (2)(a).

Taking of samples from Garda Síochána personnel for elimination (crime scene investigators) index

42. (1) A sample taken under this section from a person shall be used to generate a DNA profile in respect of the person to be entered in the elimination (crime scene investigators) index of the DNA Database System for the purpose, in relation to the investigation of offences, of ascertaining whether that person has contaminated a crime scene sample.

(2) A sample shall be taken under this section from any of the following who is assigned to duties relating to the investigation or technical examination of crime scenes or anything found at or recovered from crime scenes:

(a) a member of the Garda Síochána who is appointed as such a member after the commencement of this section;

(b) a person who is, after the commencement of this section, admitted in accordance with the Act of 2005 to training for membership (including as a reserve member within the meaning of section 3 of that Act) of the Garda Síochána;

(c) a member of the civilian staff of the Garda Síochána who is appointed as such a member of staff after the commencement of this section.

(3) A sample may be taken under this section from any of the following who is assigned to duties relating to the investigation or technical examination of crime scenes or anything found at or recovered from crime scenes only if he or she consents in writing to having such a sample taken from him or her:

(a) a member of the Garda Síochána who is such a member upon the commencement of this section;

(b) a person who is, on the commencement of this section, admitted in accordance with the Act of 2005 to training for membership (including as a reserve member within the meaning of section 3 of that Act) of the Garda Síochána;

(c) a member of the civilian staff of the Garda Síochána who is such a member of staff upon the commencement of this section.

(4) A member of the Garda Síochána or an authorised person shall inform a person to whom this section applies of the following before taking, or causing to be taken, a sample under this section from him or her:

(a) that the sample is to be taken from him or her under this section;

(b) in a case in which a sample already taken under this section from the person has proved to be insufficient or was inadequately labelled or for any other reason mentioned in section 47(1) a second or further sample under this section is required to be taken from him or her—

(i) that the first-mentioned sample has proved to be insufficient, was inadequately labelled or that other reason for requiring a second or further sample under this section to be taken, as may be appropriate, and

(ii) that a second or further sample under this section is, in accordance with section 47(1), to be taken from him or her;

(c) that the sample will be used to generate a DNA profile in respect of the person to be entered in the elimination (crime scene investigators) index of the DNA Database System and the effect of such an entry;

(d) that if, in the case of a person referred to in paragraph (a) or (b) of subsection (2) or paragraph (a) or (b) of subsection (3), the person is no longer assigned to duties relating to the investigation or technical examination of crime scenes or anything found at or recovered from crime scenes, the DNA profile in respect of the person will be transferred from the elimination (crime scene investigators) index to the elimination (Garda Síochána) index of the DNA Database System;

(e) that, in the case of a person referred to in subsection (2)(b) or (3)(b), if he or she is at any time after the taking of the sample appointed as a member of the Garda Síochána, the DNA profile

generated from the sample in respect of the person and entered in the elimination (crime scene investigators) index of the DNA Database System may be retained in that index of that System in accordance with subsection (8); and
(f) that the sample may be destroyed, and the DNA profile in respect of the person entered in the elimination (crime scene investigators) index or the elimination (Garda Síochána) index, as the case may be, of the DNA Database System may be removed from that System, in accordance with Part 10.
(5) Subject to this Act, a member of the Garda Síochána or an authorised person may take, or cause to be taken, a sample under this section from a person to whom this section applies.
(6) A sample that was taken before the commencement of this section from a person referred to in subsection (3) for the purpose, in relation to the investigation of offences, of ascertaining whether that person has contaminated a crime scene sample, and any DNA profile that was generated from the sample in respect of the person, shall be regarded as a sample taken from him or her under this section and a DNA profile generated from the sample to be entered in the elimination (crime scene investigators) index of the DNA Database System in respect of him or her only if—
(a) that person consents in writing to the sample and DNA profile concerned being so regarded, and
(b) before the consent referred to in paragraph (a) is obtained, subsection (4) shall, with any necessary modifications, be applied in relation to that person.
(7) If a person referred to in paragraph (a) or (b) of subsection (2), or paragraph (a) or (b) of subsection (3), from whom a sample was taken, or is regarded under subsection (6) as having been taken, under this section is no longer assigned to duties relating to the investigation or technical examination of crime scenes or anything found at or recovered from crime scenes, the DNA profile that was generated from the sample in respect of the person shall be transferred from the elimination (crime scene investigators) index to the elimination (Garda Síochána) index of the DNA Database System.
(8) If a person referred to in subsection (2)(b) or (3)(b) is at any time after a sample is taken, or in the case of a person referred to in subsection (3)(b) is regarded under subsection (6) as having been taken, from him or her under this section appointed as a member of the Garda Síochána, the DNA profile generated from the sample in respect of the person and entered in the elimination (crime scene investigators) index of the DNA Database System may be retained in that index of that System as if it were generated from a sample taken from the person under subsection (2)(a).
Taking of samples from members of staff of FSI for elimination (crime scene investigators) index
43. (1) A sample taken under this section from a member of the staff of FSI shall be used to generate a DNA profile in respect of the member of staff to be entered in the elimination (crime scene investigators) index of the DNA Database System for the purpose, in relation to the investigation of offences, of ascertaining whether that member of staff has contaminated a crime scene sample.
(2) A sample shall be taken under this section from a member of the staff of FSI who is appointed as such a member of staff after the commencement of this section.
(3) A sample may be taken under this section from a member of the staff of FSI who is such a member of staff upon the commencement of this section only if he or she consents in writing to having such a sample taken from him or her.
(4) A person who is authorised in writing by the Director of FSI to take samples under this section shall inform a member of the staff of FSI of the following before taking, or causing to be taken, such a sample from him or her:
(a) that the sample is to be taken from him or her under this section;
(b) in a case in which a sample already taken under this section from the member of staff has proved to be insufficient or was inadequately labelled or for any other reason mentioned in section 47(2) a second or further sample under this section is required to be taken from him or her—
(i) that the first-mentioned sample has proved to be insufficient, was inadequately labelled or that other reason for requiring a second or further sample under this section to be taken, as may be appropriate, and

(ii) that a second or further sample under this section is, in accordance with section 47(2), to be taken from him or her;
(c) that the sample will be used to generate a DNA profile in respect of the person to be entered in the elimination (crime scene investigators) index of the DNA Database System and the effect of such an entry; and
(d) that the sample may be destroyed, and the DNA profile in respect of the person entered in the elimination (crime scene investigators) index of the DNA Database System may be removed from that System, in accordance with Part 10.
(5) Subject to this Act, a person who is authorised in writing by the Director of FSI to take samples under this section may take, or cause to be taken, such a sample from a member of the staff of FSI.
(6) A sample that was taken from a member of the staff of FSI before the commencement of this section for the purpose, in relation to the investigation of offences, of ascertaining whether that member of staff has contaminated a crime scene sample, and any DNA profile that was generated from the sample in respect of the member of staff, shall be regarded as a sample taken from him or her under this section and a DNA profile generated from the sample to be entered in the elimination (crime scene investigators) index of the DNA Database System in respect of him or her only if—
(a) that member of staff consents in writing to the sample and DNA profile concerned being so regarded, and
(b) before the consent referred to in paragraph (a) is obtained, subsection (4) shall, with any necessary modifications, be applied in relation to that member of staff.
Taking of samples from other persons for elimination purposes
44. (1) A sample taken under regulations made under this section from a person prescribed under subsection (2) (in this section called a "prescribed person") shall be used to generate a DNA profile in respect of the prescribed person for the purpose, in relation to the investigation of offences, of ascertaining whether that person has contaminated a crime scene sample.
(2) Any of the following persons may be prescribed for the purposes of this section:
(a) such officers of the Minister who are assigned to perform duties in the State Pathologist's Office of the Department of Justice and Equality as the Minister considers appropriate to prescribe;
(b) such members of the staff of the Ombudsman Commission as the Minister considers appropriate to prescribe;
(c) such other persons, or class of persons, as the Minister considers appropriate to prescribe who, by reason of the functions or tasks performed or carried out by them, may inadvertently contaminate crime scene samples.
(3) The Minister may, in relation to prescribed persons, prescribe all or any of the following:
(a) the circumstances in which samples shall be, or may be, taken from such persons;
(b) the arrangements to be made for the taking of samples from such persons;
(c) the information to be given to such persons before samples are taken from them;
(d) the circumstances in which the consent of such persons is required before samples are taken from them;
(e) the circumstances in which samples may be re-taken from such persons;
(f) the circumstances in which DNA profiles in respect of such persons generated from the samples taken from them may be—
(i) entered in the elimination (crime scene investigators) index of the DNA Database System,
(ii) entered in the elimination (prescribed persons) index of that System,
(iii) transferred to the elimination (crime scene investigators) index from the elimination (prescribed persons) index of that System or from the former index to the latter index of that System, or
(iv) used, without entering them in the DNA Database System, to ascertain whether such persons have contaminated particular crime scene samples;
(g) subject to section 90, the circumstances in which samples taken from such persons may be destroyed and the DNA profiles in respect of such persons generated from those samples may be removed from the DNA Database System or destroyed, as may be appropriate.

(4) Regulations made by the Minister under this section may prescribe different circumstances and different arrangements for the taking or re-taking of samples or the destruction of samples or the destruction, or removal from the DNA Database System, of DNA profiles in accordance with this section in respect of different prescribed persons or different classes of such persons.

Direction from Commissioner for sample to be taken for elimination purposes

45. (1) If the Commissioner has good reason to believe that, in relation to the investigation of an offence, a person specified in subsection (2) has, or may have, contaminated a particular crime scene sample, the Commissioner may direct that the person shall have a sample taken from him or her under this section for the purpose, in relation to the investigation of that offence, of ascertaining whether that person has contaminated that crime scene sample.

(2) A direction may be given under subsection (1) in respect of any of the following persons, other than a person to whom section 41(2) or 42(2) applies:

(a) a member of the Garda Síochána;

(b) a person who is in accordance with the Act of 2005 admitted to training for membership (including as a reserve member within the meaning of section 3 of that Act) of the Garda Síochána;

(c) a member of the civilian staff of the Garda Síochána.

(3) A direction under subsection (1) shall be given in writing and the Commissioner shall give, or cause to be given, a copy of it to the person to whom it relates.

(4) A member of the Garda Síochána or an authorised person shall inform a person of the following before taking, or causing to be taken, a sample under this section from him or her:

(a) that the sample is to be taken from him or her pursuant to a direction given under this section;

(b) in a case in which a sample already taken under this section from the person has proved to be insufficient or was inadequately labelled or for any other reason mentioned in section 47(1) a second or further sample under this section is required to be taken from him or her—

(i) that the first-mentioned sample has proved to be insufficient, was inadequately labelled or that other reason for requiring a second or further sample under this section to be taken, as may be appropriate, and

(ii) that a second or further sample under this section is, in accordance with section 47(1), to be taken from him or her;

(c) that the sample will be used to generate a DNA profile in respect of the person for the purpose of ascertaining whether he or she has contaminated the crime scene sample concerned;

(d) that the sample, and the DNA profile in respect of the person generated from it, may be destroyed in accordance with Part 10.

(5) Subject to this Act, a member of the Garda Síochána or an authorised person may take, or cause to be taken, a sample under this section from a person in respect of whom a direction is given under subsection (1).

Direction from Director of FSI for sample to be taken for elimination purposes

46. (1) If the Director of FSI has good reason to believe that, in relation to the investigation of an offence, a person specified in subsection (2) has, or may have, contaminated a particular crime scene sample, the Director may direct that the person shall have a sample taken from him or her under this section for the purpose, in relation to the investigation of that offence, of ascertaining whether that person has contaminated that crime scene sample.

(2) A direction may be given under subsection (1) in respect of a member of the staff of FSI other than a member of staff to whom section 43(2) applies.

(3) A direction under subsection (1) shall be given in writing and the Director of FSI shall give, or cause to be given, a copy of it to the member of the staff of FSI to whom it relates.

(4) A person who is authorised in writing by the Director of FSI to take samples under this section shall inform a member of the staff of FSI of the following before taking, or causing to be taken, such a sample from him or her:

(a) that the sample is to be taken from him or her pursuant to a direction given under this section;

(b) in a case in which a sample already taken under this section from the member of staff has proved to be insufficient or was inadequately labelled or for any other reason mentioned in section 47(2) a second or further sample under this section is required to be taken from him or her—

(i) that the first-mentioned sample has proved to be insufficient, was inadequately labelled or that other reason for requiring a second or further sample under this section to be taken, as may be appropriate, and

(ii) that a second or further sample under this section is, in accordance with section 47(2), to be taken from him or her;

(c) that the sample will be used to generate a DNA profile in respect of the member of staff for the purpose of ascertaining whether he or she has contaminated the crime scene sample concerned;

(d) that the sample, and the DNA profile in respect of the member of staff generated from it, may be destroyed in accordance with Part 10.

(5) Subject to this Act, a person who is authorised in writing by the Director of FSI to take samples under this section may take, or cause to be taken, such a sample from a person in respect of whom a direction is given under subsection (1).

Re-taking of samples under Part 5

47. (1) Where a sample taken from a person under section 41, 42 or 45 proves to be insufficient or was inadequately labelled or, for any other good reason, the Commissioner considers that it is necessary for a second or further such sample to be taken from the person, a second or further sample may be taken from him or her in accordance with whichever of those sections is appropriate.

(2) Where a sample taken from a person under section 43 or 46 proves to be insufficient or was inadequately labelled or, for any other good reason, the Director of FSI considers that it is necessary for a second or further such sample to be taken from the person, a second or further sample may be taken from him or her in accordance with whichever of those sections is appropriate."

Annex N: Examples of Legal Provisions Restricting Forensic DNA Profiles to Non-Coding DNA

The Criminal Justice (Forensic Evidence and DNA Database System) Act 2014, Ireland[260] states in Article 2: *"DNA profile", in relation to a person, means information comprising a set of identification characteristics of the non-coding part of DNA derived from an examination and analysis of a sample of biological material that is clearly identifiable as relating to the person and that is capable of comparison with similar information derived from an examination and analysis of another sample of biological material for the purpose of determining whether or not that other sample could relate to that person*..

Russian law refers to: "*genomic information - personal data, including encoded information of specific fragments of deoxyribonucleic acid of an individual or an unidentified corpse, which do not characterize their physiological characteristics*". Federal Law of the Russian Federation dated December 3, 2008 N 242-FZ 'On State Genomic Registration in the Russian Federation'.[261]
In Brazil, the law states: "*The genetic information contained in the databases of genetic profiles may not reveal somatic or behavioral traits of people, except genetic determination of gender, according to constitutional and international human rights, human genome and genetic data*." Article 2, Bill n. 2458/2011.[262]

In the European Union (EU), the Prüm Decisions, which allow sharing of DNA matches between EU Member States, state:
"*For the purpose of implementing this Decision, the Member States shall ensure the availability of reference data from their national DNA analysis files as referred to in the first sentence of paragraph 1. Reference data shall only include DNA profiles established from the non-coding part of DNA and a reference number. Reference data shall not contain any data from which the data subject can be directly identified. Reference data which is not attributed to any individual (unidentified DNA profiles) shall be recognisable as such.* " Article 1(2), European Council Decision 2008/615/JHA.[263]

Argentina's law states:
"*For the purposes of this standard "genetic fingerprint" shall mean an alphanumeric registration made exclusively on the basis of genotypes that segregate independently, are polymorphic in the population, lack direct association in gene expression and contribute only identifying information*".[264]

Belgium's law[265] defines a DNA profile as: "*a specific alphanumeric code to each individual and drawn exclusively from non-coding sequences of the gene pool*".

In Germany, the law on the data of DNA analysis states[266]: "*(2) The data manager shall process personal data in connection with only such DNA characteristics which are necessary for the identification of a person or the assignment of a trace to a particular person (DNA identification pattern). The storage of personal data in connection with other features or combinations of features from the coding region of DNA allow the creation of a personal profile (genetic systems), is inadmissible*". (Section 2.2)

In Portugal, Article 12 (1) states[267]:
"*The sample analysis is restricted to only those DNA markers that are absolutely necessary for the identification of the holder for the purposes of this Act*".

The Republic of Korea's law states in Article 2[268]:

"*3. The term "DNA identification" means acquiring DNA identification information by examining and analyzing a specific part of DNA base sequence, not containing genetic information, for the purpose of identification of an individual;*
4. The term "DNA identification information" means information acquired through a DNA identification process for the purpose of identification of an individual, which is indicated by a combination of serial numbers or codes";
And in Article 3(2):
"*DNA identification information stored in the database shall not include any information or personal data, other than matters necessary for identification of an individual*".

South Africa's Law states in Article 1(e)[269]:
"(fC)'forensic DNA analysis' means the analysis of sections of the DNA of a bodily sample or crime scene sample to determine the forensic DNA profile: Provided that this does not relate to any analysis pertaining to medical tests or for health purposes or mental characteristic of a person or to determine any physical information of the person other than the sex of that person;
(fD) 'forensic DNA profile' means the results obtained from forensic DNA analysis of bodily samples taken from a person or samples taken from a crime scene, providing a unique string of alpha numeric characters to provide identity reference: Provided this does not contain any information on the health or medical condition or mental characteristic of a person or the predisposition or physical information of the person other than the sex of that person".

Annex O: Example Provisions for Missing Persons' DNA Databases

Ireland's Act uses the following definition[270]:
""missing person" means a person who, whether before or after the commencement of this section, is observed to be missing from his or her normal patterns of life, in relation to whom those persons who are likely to have heard from the person are unaware of the whereabouts of the person and that the circumstances of the person being missing raises concerns for his or her safety and well-being".

In the UK: "*In certain circumstances, volunteer samples may also be requested from individuals, together with consent for the resulting profile to be searched and retained on a DNA database. Such samples are only requested in a relatively small number of cases, for example, in missing persons enquiries and from potential vulnerable persons. Where consent to retention is also provided, these volunteer profiles will be loaded to the Missing Persons DNA Database (MPDD) or the Vulnerable Persons Database (VPDD). Volunteer samples are also sometimes taken from previously unsampled registered sex offenders and the resulting profiles are loaded to the NDNAD* [National DNA Database]" (para 2.10 UK NDNAD biennial report 2009-11).[271]

The FBI administers the National Missing Person DNA Database (NMPDD) as part of the National DNA Index System (NDIS). The NMPDD compares DNA records stored in the Missing Person, Relatives of Missing Person, and Unidentified Human Remains Indexes of NDIS.[272] US law states[273]:
"*(a) In general*
The Attorney General shall make grants to promote the use of forensic DNA technology to identify missing persons and unidentified human remains.
(b) Requirement
Each State or unit of local government that receives funding under this section shall be required to submit the DNA profiles of such missing persons and unidentified human remains to the National Missing Persons DNA Database of the Federal Bureau of Investigation.
(c) Authorization of appropriations
There are authorized to be appropriated $2,000,000 for each of fiscal years 2005 through 2009 to carry out this section".

Portugal's DNA law states[274]:
"*Article 20*
Data Interconnection within the base
DNA profile data
1 - DNA profiles obtained from samples taken from the accused under the provisions of paragraph 1 Article 8, can be compared with the data contained in the files provided for in paragraphs b), d) and f) of paragraph 1 of Article 15
2 - DNA profiles obtained from samples taken from relatives, pursuant to paragraph 2 of Article 7 as well as profiles for the "reference samples" of missing persons received under paragraph 1 of article 7, can only be compared with the estimated file in paragraph b) of paragraph 1 of Article 15
3 - DNA profiles obtained from samples collected from volunteers, under Article 6, may be compared with any of the profiles entered in files set out in paragraph 1 of article 15
4 - DNA profiles obtained from the unidentified samples collected at the crime scene under paragraph 4 of Article 8 and the DNA profiles of people convicted in criminal cases in accordance with paragraphs 2 and 3 Article 8, can be compared with the data contained the files provided for in a), b), d), e) and f) of paragraph 1
Article 15

5 - Exceptionally, by reasoned request, there may be other data comparisons not mentioned in this article by prior assent of the supervisory board and the CNPD."

Annex P: Example Legal Provisions on Governance of Forensic DNA Databases

Portugal's DNA law states[275]:
Supervisory board database
DNA profiles
Article 29
Nature and composition
1 - Control of DNA profile database is made by the Supervisory Board, appointed by the Assembly of the Republic, without prejudice to the supervisory powers this sovereign body, in constitutional terms.
2 - The Supervisory Board is an administrative entity independent authority with powers of responding only to the Parliament.
3 - The supervisory board consists of three citizens of recognized suitability and the full enjoyment of civil and political rights and is incompatible with the exercise of supervisory board member activity, membership of other boards or committees with oversight functions or control of a similar nature.
4 - The members of the supervisory board are appointed by Parliament, according to the method of Hondt highest average for a term of four years.
5 - The members of the supervisory board should be included in a list published in the 1st Series of the Official Gazette.
6 - The members of the supervisory board take office before the National Assembly, within 10 days of the publication of the list referred to in the preceding paragraph, and may resign from office by written declaration, submitted to the President of Parliament, the which is published in the 2nd series of the State Gazette."
And:
Article 30
Competence and functioning
1 - The status of the members of the supervisory board ensures the independence of the exercise of their duties and consists of natural law, to be published within six months after the entry into force of this law.
2 - It is the responsibility of the Supervisory Board:
a) To authorize such acts, where so provided in this law;
b) issue an opinion on the operating rules of the database, when the same subject is approved or changed and on any other matters where so requested;
c) Request and obtain clarifications and information, by the INML where it deems it necessary to complete exercising its supervisory powers;
d) Get the INML and medical-legal advice clarifications needed on specific issues."

The Republic of Korea's law states[276]:
"*Article 14 (Managing Committee of DNA Identification Information Database)*
(1) The Managing Committee of DNA Identification Information Database (hereinafter referred to as the "Committee") shall be established under the jurisdiction of the Prime Minister in order to require the Committee to deliberate on the following matters regarding the management and operation of the database:
1. Matters concerning the collection, transportation, storage, and destruction of DNA samples;
2. Matters concerning the method of, and procedure for, DNA identification and the standardization of identification technology;
3. Matters concerning the description of DNA identification information and the storage and erasure of the database;
4. Other matters prescribed by Presidential Decree.

(2) The Committee shall be comprised of not less than seven, but not more than nine members, including one Chairperson;
(3) Committee members shall be commissioned by the Prime Minister from among the following persons, while the Chairperson shall be appointed by the Prime Minister from among committee members:
1. Grade-V or higher-ranking public officials (including public officials in general service, who are members of the Senior Executive Service) or persons who are, or have been, in an equivalent position in a public institution and who have experience in DNA-related work;
2. Persons who serve, or have served, as an adjunct or higher professor or with an equivalent position in a university or an officially recognized research institute and who have special knowledge and ample experience in research on bioscience or medicine;
3. Other persons who have ample knowledge and experience in ethics, social science, legal profession, or journalism.
(4) The term of office for each committee member shall be three years.
(5) If the Committee considers it necessary for deliberation on matters under subparagraphs of paragraph (1), it may request the Prosecutor General or the Commissioner General of the National Police Agency to submit relevant data, and may require the person in charge of DNA identification information to attend the Committee's meetings to hear his/her opinion.
(6) The Committee may present its opinion on matters, on which it has deliberated upon pursuant to subparagraphs of paragraph (1), to the Prosecutor General or the Commissioner General of the National Police Agency.
(7) Necessary matters concerning the organization and operation of the Committee shall be prescribed by Presidential Decree, in addition to matters provided for in paragraphs (1) through (6)."

Ireland's law states[277]:
"*DNA Database System Oversight Committee*
71. (1) Upon the commencement of this section, a committee which shall be known as An Coiste Formhaoirsithe um an gCóras Bunachair Sonraí DNA or, in the English language, as the DNA Database System Oversight Committee (in this Act referred to as "the Committee") shall stand established to perform the functions assigned to it by this Act.
(2) Subject to this Part, the Committee shall be independent in the performance of its functions.
(3) Schedule 1 shall have effect in relation to the Committee.
Functions of Committee
72. (1) The Committee shall oversee the management and operation of the DNA Database System for the purposes of maintaining the integrity and security of the System and shall, for those purposes, satisfy itself that the provisions of this Act in relation to the System are being complied with.
(2) Without prejudice to the generality of subsection (1), the Committee shall oversee—
(a) the arrangements employed by the Director of FSI in relation to the receipt, handling, transmission and storage of samples taken under this Act for the purpose of generating DNA profiles for entry in the DNA Database System,
(b) the procedures employed by the Director of FSI in relation to the generation of DNA profiles from the samples taken under this Act, and the quality control and quality assurance of those procedures, to ensure that they comply with international best practice,
(c) the measures employed by the Director of FSI to ensure that the DNA Database System is not improperly accessed by any person, that the DNA profiles and information entered in the System are used only for the purposes permitted by this Act and that they are not improperly disclosed to any person,
(d) the means by which the results of searches of the DNA Database System are reported by the Director of FSI to the Garda Síochána, the Ombudsman Commission or a coroner, as may be appropriate,

(e) the practices and procedures employed by the Director of FSI to ensure that samples taken under this Act for the purpose of generating DNA profiles for entry in the DNA Database System are destroyed, and the DNA profiles generated from those samples are removed from that System, in accordance with Part 10,
(f) the practices and procedures employed by the Director of FSI in the operation of Chapters 2 and 7 of Part 12, and
(g) the practices and procedures employed by the Director of FSI in the operation of section 4.
(3) The Committee shall, in the performance of its functions under subsections (1) and (2), make such recommendations as it considers appropriate in relation to the management and operation of the DNA Database System to the Minister and the Director of FSI, as may be appropriate.
(4) The Committee may, and if so requested by the Minister shall, review any matter relating to the management and operation of the DNA Database System and shall submit a report in writing of any such review to the Minister.
(5) Subject to subsections (6) and (7), the Minister shall, as soon as practicable after receiving a report under subsection (4), cause a copy of it to be laid before each House of the Oireachtas and to be published in such manner as the Minister considers appropriate.
(6) The Minister may, when laying a copy of a report received by him or her under subsection (4) before each House of the Oireachtas or publishing the report, omit any matter from the copy of the report that is so laid or published if he or she is of opinion that the disclosure of the matter—
(a) would be prejudicial to the security of the DNA Database System, the security of the State or the investigation of criminal offences, or
(b) may infringe the constitutional rights of any person.
(7) If a matter is omitted in accordance with subsection (6) from a report received by the Minister under subsection (4), a statement to that effect shall be attached to the copy of the report when it is laid before each House of the Oireachtas or is published."

In the EU, data controllers have specific legal obligations and there are independent national supervisor authorities that can investigate complaints. The EU Data Protection Directive[278] states (48): "*Where the controller denies a data subject his or her right to information, access to or rectification or erasure of personal data or restriction of processing, the data subject should have the right to request that the national supervisory authority verify the lawfulness of the processing. The data subject should be informed of that right. Where the supervisory authority acts on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications or reviews by the supervisory authority have taken place. The supervisory authority should also inform the data subject of the right to seek a judicial remedy*" and (50) "*The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and should be able to demonstrate that processing activities are in compliance with this Directive. Such measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons*" and (53) "*In order to be able to demonstrate compliance with this Directive, the controller should adopt internal policies and implement measures, which adhere in particular the principles of data protection by design and data protection by default*". In addition, (75) "*The establishment in Member States of supervisory authorities that are able to exercise their functions with complete independence is an essential component of the protection of natural persons with regard to the processing of their personal data*" and (81) "*Each supervisory authority should handle complaints lodged by any data subject and should investigate the matter or transmit it to the competent supervisory authority. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory*

authority, intermediate information should be provided to the data subject" and (85) "*Every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy in accordance with Article 47 of the Charter where the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject*" and (86) "*Each natural or legal person should have the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person*".

Article 10 states, regarding processing of special categories of personal data:

"*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject*".

Article 17 provides for the exercise of rights by the data subject and verification by the supervisory authority. Article 19 specifies the obligations of the controller. Article 24 requires the controller to keep records of data processing activities and Article 25 to log activities such as the erasure of records. Article 32 states that Member States shall provide that the controller designates a data protection officer to monitor compliance with the Directive. Articles 41 to 49 cover the role of the independent supervisory authorities.

The US state of Maryland requires an annual report on the status and performance of the state's DNA database[279]:

"*§ 2-513. Annual report*

(a) In general. --

(1) (i) On or before April 1, 2010, and on or before April 1 annually thereafter, the Department shall report to the Governor and, in accordance with § 2-1246 of the State Government Article, the General Assembly, on the status of the statewide DNA data base system as specified in subsection (b) of this section.

(ii) On or before January 31, 2010, and on or before January 31 annually thereafter, local law enforcement agencies shall report to the Department for the preceding calendar year with the information necessary for the Department to comply with the requirements of subsection (b) of this section.

(2) The annual report shall be posted on the Department website on or before April 1 of each year.

(b) Contents. -- The annual report shall include, for the preceding calendar year:

(1) total expenses incurred for the operation and management of the DNA data base and DNA testing program, specifying the actual and human resource costs of DNA collection and transport, DNA analyses, data base operation and oversight, and State laboratory personnel and maintenance;

(2) total funding provided by the State to each forensic crime laboratory in the preceding year;

(3) a statistical analysis of the racial demographics of individuals who have been charged with a crime of violence or burglary, or attempt to commit a crime of violence or burglary, as defined in § 2-501 of this subtitle;

(4) the number of DNA samples collected from individuals charged with a crime of violence or burglary, or attempt to commit a crime of violence or burglary, as defined in § 2-501 of this subtitle;

(5) the sufficiency of protocols and procedures adopted to prevent the unlawful testing of DNA and ensure the expungement of DNA as required under this subtitle; and

(6) a detailed analysis of the investigations aided by DNA profiles that includes:

(i) the number of matches;
(ii) the number of matches that resulted in investigation of the person identified;
(iii) the number of matches that resulted in formal charges;
(iv) the number of matches that resulted in convictions;
(v) the number of matches that resulted in exonerations;
(vi) the number of matches that resulted in convictions for persons not already incarcerated; and
(vii) the prior offenses for which a person has been convicted where a match occurred".

Annex Q: Example Provisions for Security of Data

The EU Data Protection Directive[280] states (28) "*In order to maintain security in relation to processing and to prevent processing in infringement of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, including by preventing unauthorised access to or use of personal data and the equipment used for the processing, and that takes into account available state of the art and technology, the costs of implementation in relation to the risks and the nature of the personal data to be protected*" and (60) "*In order to maintain security and to prevent processing that infringes this Directive, the controller or processor should evaluate the risks inherent in the processing and should implement measures to mitigate those risks, such as encryption. Such measures should ensure an appropriate level of security, including confidentiality and take into account the state of the art, the costs of implementation in relation to the risk and the nature of the personal data to be protected*". Article 4(1)(f)states that personal data must be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*". Article 20 specifies requirements for data protection by design and by default. Article 29 requires measures for the security of processing and Articles 30 and 31 require notifications of data breaches.

In Germany, the law on the data of DNA analysis states[281]: "*10.5 The access rights to data in the "DNA analysis file" will be allocated in the data processing system so that modification or deletion of data shall be carried out exclusively by authorized staff of the authority which has entered the data (storage control, see. S 11 para. 3 BKAG)*". Also[282]:
" *10.6 The transfer of data is carried out exclusively for legitimate queries from data terminals through specially protected dedicated transmission paths between the State Criminal Police Offices and the Federal Criminal Police Office (transmission control).*"

Portugal's DNA law states[283]:
"*Article 27*
Information security
1 - The database guarantees should be conferred by security required to prevent the consultation, modification, suppression, the addition of the destruction or data communication when it is not allowed by this law.
2 – To be monitored, with a view to the safety of information, are:
a) the media and their transport in order to prevent them from being read, disclosed, copied, modified or deleted by any person or order not allowed to do so;
b)the insertion of data in order to prevent the introduction, and any taking of knowledge, dissemination, unauthorized modification or deletion of personal data;
c) data processing systems, to prevent them being used by unauthorized persons through data transmission facilities;
d) access to data so that authorized persons can only have access to data when pursuing their legal duties;
e) the transmission of data to ensure that their use is limited to authorized entities;
f) the introduction of personal data in treatment systems, in order to verify that data has been entered, when and by whom.
3 - To maintain security and loyalty conditions the storage and processing of data, the performance of technical functions of collecting and analyzing samples DNA and other comparable function involving the direct contact with carriers of genetic data, is subject to the provisions of subparagraph b) of paragraph 1 of Article 18".

Malaysia's DNA law states[284]:

"*Access of DNA profile or information*
11. (1) The access to, a communication or use of DNA profiles or any information in relation thereto stored in the DNA Databank by the Head of DNA Databank, Deputy Head of DNA Databank, DNA Databank officers and any chemist shall only for the purposes of—

(a) forensic comparison with any other DNA profiles or information in the course of an investigation of any offence conducted by any enforcement agency;
(b) administering the DNA Databank; or
(c) making the information available to the person to whom the information relates.
(2) For the avoidance of doubt, the access to, a communication or use of DNA profiles or any information in relation thereto under subsection (1) by a chemist shall only be for the purpose mentioned in paragraph (a) of that subsection."

Annex R: Examples of Provisions Restricting the Uses of Forensic DNA Databases

Germany's criminal law states: "*The data may be transmitted only for the purposes of criminal proceedings, for threat prevention and for international mutual legal assistance in respect thereof*".[285] (Section81g). Germany's law on the data of DNA analysis states[286]: "*2.2 (1) The "DNA analysis file" is used to pre-empt future of offenses of considerable importance, especially of crimes and offenses against sexual self-determination, dangerous bodily harm, theft in particularly severe cases, or extortion*" and "*2.3 The file enables*
• *the identification of relevant persons*
• *the assignment of persons to crime scenes*
• *the assignment of a crime scene to another crime scene*
• *police and criminal intelligence*
• *the elimination of insignificant information and intelligence*
• *the elimination of non-suspects*".

Belgium's law states[287]: "*Art. 3. 1 § 1. Without prejudice to what is provided in § 2, DNA and DNA profiles comparison analysis can only be performed in the context of criminal proceedings, to allow direct or indirect identification of individuals involved in the commission of an offense to remove suspicions about others or to prove their innocence.*
§ 2. However, DNA and DNA profiles comparison analysis can also be performed to allow direct or indirect identification of unknown deceased and facilitate the search for missing persons."

US Federal law states that the DNA database shall be[288]:
"*(3) maintained by Federal, State, and local criminal justice agencies (or the Secretary of Defense in accordance with section 1565 of title 10) pursuant to rules that allow disclosure of stored DNA samples and DNA analyses only—*
(A) to criminal justice agencies for law enforcement identification purposes;
(B) in judicial proceedings, if otherwise admissible pursuant to applicable statutes or rules;
(C) for criminal defense purposes, to a defendant, who shall have access to samples and analyses performed in connection with the case in which such defendant is charged; or
(D) if personally identifiable information is removed, for a population statistics database, for identification research and protocol development purposes, or for quality control purposes".

Annex S: Example Provisions Restricting Research Uses of Forensic DNA Databases

Portugal's DNA law states[289]:
"*Article 23*
Information for statistical purposes or scientific research
1 - Information obtained from the DNA profiles can be communicated for scientific research or statistics, after irreversible anonymisation.
2 - The irreversible anonymisation process data should be performed so that it is no longer possible identify the data subject, not allowing any type of nominal or alphanumeric search."

US Federal law states that the DNA database shall be used for research only[290]:
"*(3)(D) if personally identifiable information is removed, for a population statistics database, for identification research and protocol development purposes, or for quality control purposes*".

Annex T: Example Provisions on the Use of Familial Searching

Dutch law contains the following provisions on the use of familial DNA searching[291]:
"*Article 151da*
1. Notwithstanding Article 21, fourth paragraph, of the Data Protection Act, the Public Prosecutor in the interest of the study recommended that a DNA research is aimed at establishing kinship. If the DNA test is performed using the DNA profiles, in accordance with this Code, the Data Protection Act and the Act to study DNA-convicts are processed, can be ordered only after written authorization from the judge to application of the Prosecutor. Article 151a, second paragraph, shall apply.
2. Cellular material that under this Code, the Data Protection Act or the Act to study DNA-convicts decreased for identifying and processing a DNA profile may be used to establish kinship. Cellular material from a known person who is not suspected of a crime, can only be purchased with his written consent and used to establish kinship.
3. The DNA test can be performed only in cases of suspicion of a crime for which the legal description of eight years imprisonment or more is made and one of the crimes described in Articles 109, 110, 141, second paragraph, under 1 °, 181, under 2 °, 182, 247, 248a, 248b, 249, 281, first paragraph, under 1 °, 290, 300, second and third paragraph, and 301, second paragraph, of the Criminal Code. If a DNA test under Article 151a, first paragraph, leads to the establishment of kinship, the prosecutor in this result the investigation use.
4. For general administrative arrangements can be made about the arrangements of the DNA testing."

In New Zealand, the legislation does not extend to providing a framework for forensic utilisation of the DNA Profile Databank (DPD). In its absence, ESR and New Zealand Police have developed agreed procedures for operational activities involving the NZ DPD, including on familial searching[292]:
"*Familial searching:*
1. A familial search of the DPD may be considered for a serious offence where there is no DNA link resulting from a specific crime profile search.
2. Familial searching does not contravene the CI (BS) Act however, it is recognised by both ESR and the NZ Police that this type of search has important ethical implications and should only be considered on a case-by-case basis.
3. As this type of search explores familial relatedness it shall only be undertaken where it is considered necessary and proportionate in a particular case.
4. NZ Police shall have an authorisation process for familial search requests to ESR which considers the seriousness of the offence and whether a familial search is appropriate for the investigation.
5. NZ Police shall provide ESR with the necessary documentation which demonstrates the search has been authorised and should proceed. Authorisation shall be via completion of the proforma "NZ Police Request for a Familial Search of the NZ DNA Profile Databank".
6. A familial search will result in a list of potential close relatives to the offender and will contain sensitive personal information.
7. The list is ranked statistically on the basis of how likely a person will be a relative of the offender. ESR shall assist NZ Police in the scientific interpretation of these results.
8. Access to this list shall be restricted to Police and ESR staff involved in the investigation.
9. ESR shall keep a record of familial search requests made by NZ Police and shall provide a summary of these in an annual NZ DNA Profile Databank Report".

Annex U: Examples of Access to Post-Conviction DNA Testing

The US state of North Carolina's legislation states[293]:
"*15A-269. Request for postconviction DNA testing.*
(a) A defendant may make a motion before the trial court that entered the judgment of conviction against the defendant for performance of DNA testing and, if testing complies with FBI requirements and the data meets NDIS criteria, profiles obtained from the testing shall be searched and/or uploaded to CODIS if the biological evidence meets all of the following conditions:
(1) Is material to the defendant's defense.
(2) Is related to the investigation or prosecution that resulted in the judgment.
(3) Meets either of the following conditions:
a. It was not DNA tested previously.
b. It was tested previously, but the requested DNA test would provide results that are significantly more accurate and probative of the identity of the perpetrator or accomplice or have a reasonable probability of contradicting prior test results.
(b) The court shall grant the motion for DNA testing and, if testing complies with FBI requirements, the run of any profiles obtained from the testing, upon its determination that:
(1) The conditions set forth in subdivisions (1), (2), and (3) of subsection (a) of this section have been met;
(2) If the DNA testing being requested had been conducted on the evidence, there exists a reasonable probability that the verdict would have been more favorable to the defendant; and
(3) The defendant has signed a sworn affidavit of innocence.
(b1) If the court orders DNA testing, such testing shall be conducted by a Crime Laboratory-approved testing facility, mutually agreed upon by the petitioner and the State and approved by the court. If the parties cannot agree, the court shall designate the testing facility and provide the parties with reasonable opportunity to be heard on the issue.
(c) In accordance with rules adopted by the Office of Indigent Defense Services, the court shall appoint counsel for the person who brings a motion under this section if that person is indigent. If the petitioner has filed pro se, the court shall appoint counsel for the petitioner in accordance with rules adopted by the Office of Indigent Defense Services upon a showing that the DNA testing may be material to the petitioner's claim of wrongful conviction.
(d) The defendant shall be responsible for bearing the cost of any DNA testing ordered under this section unless the court determines the defendant is indigent, in which event the State shall bear the costs.
(e) DNA testing ordered by the court pursuant to this section shall be done as soon as practicable. However, if the court finds that a miscarriage of justice will otherwise occur and that DNA testing is necessary in the interests of justice, the court shall order a delay of the proceedings or execution of the sentence pending the DNA testing.
(f) Upon receipt of a motion for postconviction DNA testing, the custodial agency shall inventory the evidence pertaining to that case and provide the inventory list, as well as any documents, notes, logs, or reports relating to the items of physical evidence, to the prosecution, the petitioner, and the court.
(g) Upon receipt of a motion for postconviction DNA testing, the State shall, upon request, reactivate any victim services for the victim of the crime being investigated during the reinvestigation of the case and pendency of the proceedings.
(h) Nothing in this Article shall prohibit a convicted person and the State from consenting to and conducting postconviction DNA testing by agreement of the parties, without filing a motion for postconviction testing under this Article. (2001-282, s. 4; 2007-539, s. 3; 2009-203, s. 5; 2011-326, s. 12(d); 2013-360, s. 17.6(k).)".

The US state of Tennessee includes the following provision[294]:

"*40-30-304. Court order if probable that exculpatory results would not have resulted in prosecution or conviction.*

After notice to the prosecution and an opportunity to respond, the court shall order DNA analysis if it finds that:

(1) A reasonable probability exists that the petitioner would not have been prosecuted or convicted if exculpatory results had been obtained through DNA analysis;

(2) The evidence is still in existence and in such a condition that DNA analysis may be conducted;

(3) The evidence was never previously subjected to DNA analysis or was not subjected to the analysis that is now requested which could resolve an issue not resolved by previous analysis; and

(4) The application for analysis is made for the purpose of demonstrating innocence and not to unreasonably delay the execution of sentence or administration of justice".

The US state of Missouri has legislation which states[295]:

"*§547.035. Postconviction DNA testing for persons in the custody of the department--motion, contents--procedure*

1. A person in the custody of the department of corrections claiming that forensic DNA testing will demonstrate the person's innocence of the crime for which the person is in custody may file a postconviction motion in the sentencing court seeking such testing. The procedure to be followed for such motions is governed by the rules of civil procedure insofar as applicable.

2. The motion must allege facts under oath demonstrating that:

(1) There is evidence upon which DNA testing can be conducted; and

(2) The evidence was secured in relation to the crime; and

(3) The evidence was not previously tested by the movant because:

(a) The technology for the testing was not reasonably available to the movant at the time of the trial;

(b) Neither the movant nor his or her trial counsel was aware of the existence of the evidence at the time of trial; or

(c) The evidence was otherwise unavailable to both the movant and movant's trial counsel at the time of trial; and

(4) Identity was an issue in the trial; and

(5) A reasonable probability exists that the movant would not have been convicted if exculpatory results had been obtained through the requested DNA testing.

3. Movant shall file the motion and two copies thereof with the clerk of the sentencing court. The clerk shall file the motion in the original criminal case and shall immediately deliver a copy of the motion to the prosecutor.

4. The court shall issue to the prosecutor an order to show cause why the motion should not be granted unless:

(1) It appears from the motion that the movant is not entitled to relief; or

(2) The court finds that the files and records of the case conclusively show that the movant is not entitled to relief.

5. Upon the issuance of the order to show cause, the clerk shall notify the court reporter to prepare and file the transcript of the trial or the movant's guilty plea and sentencing hearing if the transcript has not been prepared or filed.

6. If the court finds that the motion and the files and records of the case conclusively show that the movant is not entitled to relief, a hearing shall not be held. If a hearing is ordered, counsel shall be appointed to represent the movant if the movant is indigent. The hearing shall be on the record. Movant need not be present at the hearing. The court may order that testimony of the movant shall be received by deposition. The movant shall have the burden of proving the allegations of the motion by a preponderance of the evidence.

7. The court shall order appropriate testing if the court finds:

(1) A reasonable probability exists that the movant would not have been convicted if exculpatory results had been obtained through the requested DNA testing; and

(2) That movant is entitled to relief.

Such testing shall be conducted by a facility mutually agreed upon by the movant and by the state and approved by the court. If the parties are unable to agree, the court shall designate the testing facility. The court shall impose reasonable conditions on the testing to protect the state's interests in the integrity of the evidence and the testing process.

8. The court shall issue findings of fact and conclusions of law whether or not a hearing is held".

Annex V: Examples of Safeguards for Sharing of DNA Profile Matches Overseas

The Council of Europe's modernisation of its Data Protection Convention, Chapter III - Transborder flows of personal data (Article 12) states[296]:

"*Transborder flows of personal data*

1 A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of data to a recipient who is subject to the jurisdiction of another Party to the Convention, unless the Party referred to at the beginning of the present paragraph is regulated by binding harmonised rules of protection shared by States belonging to a regional international organisation and the transfer of data is not governed by measures provided for in paragraph 3.b.

2 When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to the Convention, the transfer of data can only occur where an appropriate level of personal data protection based on the principles of the Convention is guaranteed.

3 An appropriate level of protection can be ensured by:

a) the law of that State or international organisation, including the applicable international treaties or agreements, or

b) ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.

4 Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of data may take place, if:

a) the data subject has given his/her specific, free and [explicit, unambiguous] consent, after being informed of risks arising in the absence of appropriate safeguards, or

b) the specific interests of the data subject require it in the particular case, or

c) prevailing legitimate interests, in particular important public interests, are provided by law and constitute a necessary measure in a democratic society.

5 Each Party shall provide that the competent supervisory authority within the meaning of Article 12 bis of the Convention be informed of the modalities regulating the transfers of data provided for in paragraphs 3.b when ad hoc safeguards are set up, 4.b and 4.c. It shall also provide that the supervisory authority be entitled to request that the person who transfers data, or the recipient, demonstrate the quality and effectiveness of actions taken and that the supervisory authority be entitled to prohibit, suspend or subject to condition such transfers of data".

The EU Data Protection Directive[297] states (64): "*Member States should ensure that a transfer to a third country or to an international organisation takes place only if necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and that the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer should be carried out only by competent authorities acting as controllers, except where processors are explicitly instructed to transfer on behalf of controllers. Such a transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level of protection, where appropriate safeguards have been provided, or where derogations for specific situations apply. Where personal data are transferred from the Union to controllers, to processors or to other recipients in third countries or international organisations, the level of protection of natural persons provided for in the Union by this Directive should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers or processors in the same or*

in another third country or international organisation". Articles 35 to 39 cover international transfers of personal data.

The UK Home Office has adopted a policy including requirements and principles for international exchange of DNA profiles. [298]However, this policy has not been incorporated into UK law. Amongst its requirements, the policy states that: "*outbound exchange of a DNA profile where the individual is unknown (e.g. a profile from a crime stain or an unidentified body) must always be preferred to the outbound exchange of a profile from a named individual. For example, where an unidentified deceased body is located abroad, then rather than exporting the profile of a person whose identity is known with a view to establishing if it matches a profile derived from that body, the DNA profile derived from the body should be obtained for searching against the appropriate UK DNA database(s)*".
In addition, the UK policy states: "*A named person's DNA profile should only be exported when such a course is necessary, reasonable and proportionate, is in line with s63A of PACE* [the Police and Criminal Evidence Act] *(as amended) or Section 19C of Criminal Procedure (Scotland) Act 1995 (as amended) or Article 63A PACE NI Order 1989 (as amended) and meets one or more of the following criteria:*
1 It is for purposes related to the prevention or detection of crime;
2 It is for purposes related to the identification of a deceased person;
3 It is in the interests of National Security; or
4 It is for the purposes of a Counter-Terrorism investigation."
The UK policy also states: "*An inbound named person's DNA profile will only be searched against the NDNAD with a view to establishing whether or not there is a match with a UK unidentified crime stain profile*" and "*A request to confirm the identity of a person will not be dealt with by way of a NDNAD search; any such request must be dealt with by way of a comparison of fingerprints*".

A new "umbrella agreement" has been negotiated between the EU and USA to cover data sharing for law enforcement purposes.[299,300] This agreement is not yet in force: it will be signed and formally concluded only after the US Judicial Redress Bill, granting judicial redress rights to EU citizens, has been adopted. The Council, on the basis of a proposal by the Commission, will then adopt a decision authorising the signing of the Agreement. The decision concluding the Agreement will be adopted by the Council after obtaining the consent of the European Parliament. The European Commission states that the Umbrella agreement will provide the following protections to make sure that everyone's data are protected when exchanged between police and criminal justice authorities:

"*Clear limitations on data use – Personal data may only be used for the purpose of preventing, investigating, detecting or prosecuting criminal offences, and may not be processed beyond compatible purposes.*

Onward transfer – Any onward transfer to a non-US, non-EU country or international organisation must be subject to the prior consent of the competent authority of the country which had originally transferred personal data.

Retention periods - Individuals' personal data may not be retained for longer than necessary or appropriate. These retention periods will have to be published or otherwise made publicly available. The decision on what is an acceptable duration must take into account the impact on people's rights and interests.

Right to access and rectification - Any individual will be entitled to access their personal data – subject to certain conditions, given the law enforcement context – and request it to be corrected if it is inaccurate.

Information in case of data security breaches – A mechanism will be put in place so as to ensure notification of data security breaches to the competent authority and, where appropriate, the data subject.

Judicial redress and enforceability of rights - EU citizens will have the right to seek judicial redress before US courts in case of the US authorities deny access or rectification, or unlawfully disclose their personal data".

Germany's law on the data of DNA analysis states[301]: "*7.4 (1) At the international level the BKA can conventionally transmit to police and judicial authorities information from the file as well as other information required for the prevention or prosecution of criminal offences to competent public bodies, engaged in tasks of prevention or prosecution of criminal offenses, to the extent necessary:*
1. to prosecute criminal offenses or enforcement under the rules on international legal assistance in criminal matters,
2. to avert an existing in each individual case significant threat to public safety
3. or to prevent crime of significant importance".
Germany is one of a number of countries which has signed an agreement with the United States on enhancing cooperation in preventing and combating serious crime.[302] This agreement includes provisions for automated searching of DNA profiles:
"*Article 7*
Automated searching of DNA profiles
1. If permissible under the national law of both parties and on the basis of reciprocity, the Parties may allow each other's national contact point, as referred to in Article 9, access to the reference data in their DNA analysis files, with the power to conduct automated searches by comparing DNA profiles for the investigation of serious crime. Searches maybe exercised only in individual cases and in compliance with the searching Party's national law.
2. Should an automated search show that a DNA profile supplied matches a DNA profile entered in the other Party's file, the searching national contact point shall receive by automated notification the reference data for which a match has been found. If no match can be found, automated notification of this shall be given".
This agreement includes limitations on uses:
"*Article 13*
Limitation on processing to protect personal and other data
1. Without prejudice to Article 10, paragraph 4, a Party may process data obtained under this Agreement:
a. for the purpose of its criminal investigations;
b. for preventing a serious threat to its public security;
c. in its non-criminal judicial or administrative proceedings directly related to investigations set forth in subparagraph a; or
d. for any other purpose, only with the prior consent of the Party which has transmitted the data.
2. The Parties shall not communicate data provided under this Agreement to any third State, international body or private entity without the consent of the Party that provided the data and without the appropriate safeguards.
3. A Party may conduct an automated search of the other Party's fingerprint or DNA files under Articles 4 or 7, and process data received in response to such a search, including the communication whether or not a hit exists, solely in order to:
a. establish whether the compared DNA profiles or fingerprint data match;
b. prepare and submit a follow-up request for assistance in compliance with its national law, including the legal assistance rules, if those data match; or
c. conduct record-keeping, as required or permitted by its national law.
The Party administering the file may process the data supplied to it by the searching Party during the course of an automated search in accordance with Articles 4 and 7 solely where this is necessary for the purposes of comparison, providing automated replies to the search or record-keeping pursuant to Article 15. The data supplied for comparison shall be deleted immediately following data comparison

or automated replies to searches unless further processing is necessary for the purposes mentioned under subparagraphs b. and c. of this paragraph".
And some additional safeguards regarding data protection:
"*Article 11*
Privacy and Data Protection
1. The Parties recognize that the handling and processing of personal data that they acquire from each other is of critical importance to preserving confidence in the implementation of this Agreement.
2. The Parties commit themselves to processing personal data fairly and in accord with their respective laws and:
a. ensuring that the personal data provided is adequate and relevant in relation to the specific purpose of the transfer;
b.retaining personal data only so long as necessary for the specific purpose for which the data were provided or further processed in accordance with this Agreement; and
c. ensuring that possibly inaccurate personal data is timely brought to the attention of the receiving Party in order that appropriate corrective action is taken.
3. This Agreement shall not give rise to rights on the part of any private person, including to obtain, suppress, or exclude any evidence, or to impede the sharing of personal data. Rights existing independently of this Agreement, however, are not affected".

Annex W: Examples of Penalties for Breaches of Safeguards

The Republic of Korea's law states[303]:
"*Article 17 (Penal Provisions)*
(1) A person who falsifies or alters DNA identification information shall be punished by imprisonment with prison labour for not more than seven years, or by a fine not exceeding 20 million won.
(2) A person who destroys, conceals, damages, or otherwise degrades the utility of, DNA samples collected pursuant to this Act shall be punished by imprisonment with prison labour for not more than five years, or by a fine not exceeding seven million won.
(3) A person who uses DNA samples or DNA identification information for any purpose, other than performance of his/her duties, in violation of Article 15 or provides or divulges such samples or information to another person shall be punished by imprisonment with prison labour for not more than three years, or by suspension of qualification for not more than five years.
(4) A person who falls under any of the following subparagraphs shall be punished by imprisonment with prison labour for not more than two years, or by a fine not exceeding five million won:
1. A person who inspects or acquires DNA identification information by fraud or other illegal means;
2. A person who uses DNA identification information replied pursuant to Article 11 for any purpose, other than performance of his/her duties or who provides or divulges such information to another person.
(5) A person in charge of DNA identification information shall be punished by imprisonment, with or without prison labour, for not more than one year or by suspension of qualification for not more than three years, if he/she fails to destroy DNA samples and DNA extracted therefrom or fails to erase DNA identification information, in violation of Article 12 or 13 without a justifiable ground".

Malaysia's DNA law states[304]:
"*Unauthorized use or communication of DNA profile or information*
19. (1) No person who receives a DNA profile for entry in the DNA Databank or who has access to information contained in the DNA Databank shall, except in accordance with sections 11 and 22, use or communicate such DNA profile or any information in relation thereto to be used or communicated other than for the purpose of this Act.
(2) Any person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to imprisonment for a term not exceeding five years or to a fine not exceeding fifty thousand ringgit or to both."

The EU Data Protection Directive[305] states (89): "*Penalties should be imposed on any natural or legal person, whether governed by private or public law, who infringes this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and should take all measures to implement the penalties*". Articles 52 to 57 provide for remedies, liability and sanctions.

US law states[306]:
"*(c) Criminal penalty*
A person who knowingly discloses a sample or result described in subsection (a) of this section in any manner to any person not authorized to receive it, or obtains or uses, without authorization, such sample or result, shall be fined not more than $250,000, or imprisoned for a period of not more than one year. Each instance of disclosure, obtaining, or use shall constitute a separate offense under this subsection".

References for Annexes

[199] German Code of Criminal Procedure in the version published on 7 April 1987 (Federal Law Gazette [Bundesgesetzblatt] Part I p. 1074, 1319), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I p. 410). http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf

[200] BUNDESKRIMINALAMT. Der Datenschutzbeauftragte: DNA-ANALYSE-DATEI. [In German] 29th July 2002. http://www.befreite-dokumente.de/www.befreite-dokumente.de/eingereichte-akten/einrichtungsanordnung-dna/attachment_download/publication_download.pdf

[201] Netherlands Code of Criminal Procedure [Unofficial translation] Text valid on: 08-10-2012. http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf

[202] 42 U.S. Code § 14132 - Index to facilitate law enforcement exchange of DNA identification information. https://www.law.cornell.edu/uscode/text/42/14132

[203] 42-43-44 ELIZABETH II: CHAPTER 27. An Act to amend the Criminal Code and the Young Offenders Act (forensic DNA analysis) [Assented to 13th July, 1995] http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=2328217&File=22&Language=e&Mode=1

[204] Ministerio de Justicia, Seguridad y Derechos Humanos. REGISTRO DE HUELLAS DIGITALES GENETICAS. Resolución 415/2004. 21st May 2004. http://infoleg.mecon.gov.ar/infolegInternet/anexos/95000-99999/95342/norma.htm

[205] Statutes of the Republic of Korea. Act on Use and Protection of DNA Identification Information. Act No. 9944, Jan.25, 2010. Amended by Act No.10258, Apr.15, 2010. Seoul, 2010. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/Korea_law_2010.pdf

[206] German Code of Criminal Procedure in the version published on 7 April 1987 (Federal Law Gazette [Bundesgesetzblatt] Part I p. 1074, 1319), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I p. 410). http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf

[207] 22 MARS 1999. - Loi relative à la procédure d'identification par analyse ADN en matière pénale. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1999032252&table_name=loi

[208] Netherlands Code of Criminal Procedure [Unofficial translation] Text valid on: 08-10-2012. http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf

[209] Victoria Crimes Act 1958. http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/LTObject_Store/LTObjSt6.nsf/b1612aeaf0625227ca257619000d0882/a57e26dfdab404dcca257975000569fb/$FILE/58-6231aa229A%20authorised.pdf

[210] Federal Law of the Russian Federation dated December 3, 2008 N 242-FZ "On State Genomic Registration in the Russian Federation" [Unofficial translation] http://www.rg.ru/2008/12/09/genom-registracia-dok.html

[211] German Code of Criminal Procedure in the version published on 7 April 1987 (Federal Law Gazette [Bundesgesetzblatt] Part I p. 1074, 1319), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I p. 410). http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf

[212] DEOXYRIBONUCLEIC ACID (DNA) IDENTIFICATION ACT 2009. Act 699. Malaysia.

[213] DEOXYRIBONUCLEIC ACID (DNA) IDENTIFICATION REGULATIONS 2012. Malaysia.

[214] Republic of South Africa: Act No. 37 of 2013: Criminal Law (Forensic Procedures). Amendment Act, 2013. Cape Town, 27th January 2014. http://www.justice.gov.za/legislation/acts/2013-037.pdf

[215] Statutes of the Republic of Korea. Act on Use and Protection of DNA Identification Information. Act No. 9944, Jan.25, 2010. Amended by Act No.10258, Apr.15, 2010. Seoul, 2010. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/Korea_law_2010.pdf

[216] The Human DNA Regulation Act, 2009. Tanzania. http://www.lrct.go.tz/download/laws_2009/08-2009%20The%20Human%20DNA%20Regulation%20Act,%202009%20.pdf

[217] New Zealand: Criminal Investigations (Bodily Samples) Amendment Act 2009. http://www.legislation.govt.nz/act/public/2009/0046/latest/DLM1829219.html

[218] DEOXYRIBONUCLEIC ACID (DNA) IDENTIFICATION ACT 2009. Act 699. Malaysia.

[219] DEOXYRIBONUCLEIC ACID (DNA) IDENTIFICATION REGULATIONS 2012. Malaysia.

[220] Statutes of the Republic of Korea. Act on Use and Protection of DNA Identification Information. Act No. 9944, Jan.25, 2010. Amended by Act No.10258, Apr.15, 2010. Seoul, 2010. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/Korea_law_2010.pdf

[221] BUNDESKRIMINALAMT. Der Datenschutzbeauftragte: DNA-ANALYSE-DATEI. [In German] 29th July 2002. http://www.befreite-dokumente.de/www.befreite-dokumente.de/eingereichte-akten/einrichtungsanordnung-dna/attachment_download/publication_download.pdf
[222] New Zealand: Criminal Investigations (Bodily Samples) Amendment Act 2009. http://www.legislation.govt.nz/act/public/2009/0046/latest/DLM1829219.html
[223] 2010 Maryland Code. PUBLIC SAFETY. TITLE 2 - DEPARTMENT OF STATE POLICE. Subtitle 5 - Statewide DNA Data Base System. Section 2-511 - Expungement of DNA information. http://law.justia.com/codes/maryland/2010/public-safety/title-2/subtitle-5/2-511/
[224] 2013 North Carolina General Statutes Chapter 15A - Criminal Procedure Act. Article 13 - DNA Database and Databank. http://law.justia.com/codes/north-carolina/2013/chapter-15a/article-13/
[225] Tennessee Code 40-35-321. Collection of biological specimens for DNA analysis -- Persons convicted of certain offenses -- Condition of release from imprisonment. https://www.lawserver.com/law/state/tennessee/tn-code/tennessee_code_40-35-321
[226] Missouri Revised Statutes. Chapter 650. Department of Public Safety. Section 650.055.1. August 28, 2015. Felony convictions for certain offenses to have biological samples collected, when--use of sample--highway patrol and department of corrections, duty--DNA records and biological materials to be closed record, disclosure, when--expungement of record, when. http://www.moga.mo.gov/mostatutes/stathtml/65000000551.HTML
[227] 42 U.S. Code § 14132 - Index to facilitate law enforcement exchange of DNA identification information. https://www.law.cornell.edu/uscode/text/42/14132
[228] BUNDESKRIMINALAMT. Der Datenschutzbeauftragte: DNA-ANALYSE-DATEI. [In German] 29th July 2002. http://www.befreite-dokumente.de/www.befreite-dokumente.de/eingereichte-akten/einrichtungsanordnung-dna/attachment_download/publication_download.pdf
[229] New Zealand: Criminal Investigations (Bodily Samples) Amendment Act 2009. http://www.legislation.govt.nz/act/public/2009/0046/latest/DLM1829219.html
[230] LEI Nº 12.654, DE 28 DE MAIO DE 2012. http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12654.htm
[231] New Zealand: Criminal Investigations (Bodily Samples) Amendment Act 2009. http://www.legislation.govt.nz/act/public/2009/0046/latest/DLM1829219.html
[232] Missouri Revised Statutes. Chapter 650. Department of Public Safety. Section 650.055.1. August 28, 2015. Felony convictions for certain offenses to have biological samples collected, when--use of sample--highway patrol and department of corrections, duty--DNA records and biological materials to be closed record, disclosure, when--expungement of record, when. http://www.moga.mo.gov/mostatutes/stathtml/65000000551.HTML
[233] Criminal Justice (Forensic Evidence and DNA Database System) Act 2014. Ireland. http://www.oireachtas.ie/documents/bills28/acts/2014/a1114.pdf
[234] Criminal Justice (Forensic Evidence and DNA Database System) Act 2014. Ireland. http://www.oireachtas.ie/documents/bills28/acts/2014/a1114.pdf
[235] South Australia Criminal Law (Forensic Procedures) Act 2007. https://www.legislation.sa.gov.au/LZ/C/A/CRIMINAL%20LAW%20%28FORENSIC%20PROCEDURES%29%20ACT%202007/CURRENT/2007.5.UN.PDF
[236] 42-43-44 ELIZABETH II: CHAPTER 27. An Act to amend the Criminal Code and the Young Offenders Act (forensic DNA analysis) [Assented to 13th July, 1995] http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=2328217&File=22&Language=e&Mode=1
[237] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC
[238] Criminal Justice (Forensic Evidence and DNA Database System) Act 2014. Ireland. http://www.oireachtas.ie/documents/bills28/acts/2014/a1114.pdf
[239] New South Wales Crimes (Forensic Procedures) Act 2000 No 59. http://www.legislation.nsw.gov.au/inforcepdf/2000-59.pdf?id=39c0b25c-83aa-4ce8-bd89-f62de370808c
[240] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

[241] Lei Aprova a criação de uma base de dados de perfis de ADN para fins de identificação civil e criminal. Lei n.º 5/2008, de 12 de Fevereiro. [In Portuguese] http://dre.pt/pdf1sdip/2008/02/03000/0096200968.pdf

[242] The Human DNA Regulation Act, 2009. Tanzania. http://www.lrct.go.tz/download/laws_2009/08-2009%20The%20Human%20DNA%20Regulation%20Act,%202009%20.pdf

[243] New Zealand: Criminal Investigations (Bodily Samples) Amendment Act 2009. http://www.legislation.govt.nz/act/public/2009/0046/latest/DLM1829219.html

[244] 42-43-44 ELIZABETH II: CHAPTER 27. An Act to amend the Criminal Code and the Young Offenders Act (forensic DNA analysis) [Assented to 13th July, 1995] http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=2328217&File=22&Language=e&Mode=1

[245] Republic of South Africa: Act No. 37 of 2013: Criminal Law (Forensic Procedures). Amendment Act, 2013. Cape Town, 27th January 2014. http://www.justice.gov.za/legislation/acts/2013-037.pdf

[246] FORENSIC DNA REGULATIONS, 2015. South Africa Department of Police. No. R. 207. 13th March 2015. http://www.gov.za/sites/www.gov.za/files/38561_rg_gon207.pdf

[247] HOUSE BILL 13-1020. Colorado. http://www.leg.state.co.us/clics/clics2013a/csl.nsf/fsbillcont3/81D352C1BB84F08587257AEE00570221?Open&file=1020_enr.pdf

[248] COUNCIL FRAMEWORK DECISION 2009/905/JHA on Accreditation of forensic service providers carrying out laboratory activities. 30th November 2009. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/463436/ANNEX_C_Council_Framework_Decision_2009_905_JHA.pdf

[249] https://www.gov.uk/government/organisations/forensic-science-regulator

[250] Available on: http://www.criminaljustice.ny.gov/forensic/aboutofs.htm . Accessed 10/04/14.

[251] 42 U.S. Code § 14132 - Index to facilitate law enforcement exchange of DNA identification information. https://www.law.cornell.edu/uscode/text/42/14132

[252] 42 U.S. Code § 14131 - Quality assurance and proficiency testing standards. https://www.law.cornell.edu/uscode/text/42/14131

[253] Queensland: Police Powers and Responsibilities Act 2000. https://www.legislation.qld.gov.au/legisltn/current/p/policepowresa00.pdf

[254] Council Resolution of 25 June 2001 on the exchange of DNA analysis results (2001/C 187/01). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001G0703%2801%29&from=EN

[255] Council Resolution of 30 November 2009 on the exchange of DNA analysis results. 2009/C 296/01. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009G1205%2801%29&from=EN

[256] Scientific Working Group on DNA Analysis Methods (SWGDAM). http://www.swgdam.org/

[257] Lei Aprova a criação de uma base de dados de perfis de ADN para fins de identificação civil e criminal. Lei n.º 5/2008, de 12 de Fevereiro. [In Portuguese] http://dre.pt/pdf1sdip/2008/02/03000/0096200968.pdf

[258] Republic of South Africa: Act No. 37 of 2013: Criminal Law (Forensic Procedures). Amendment Act, 2013. Cape Town, 27th January 2014. http://www.justice.gov.za/legislation/acts/2013-037.pdf

[259] Criminal Justice (Forensic Evidence and DNA Database System) Act 2014. Ireland. http://www.oireachtas.ie/documents/bills28/acts/2014/a1114.pdf

[260] Criminal Justice (Forensic Evidence and DNA Database System) Act 2014. Ireland. http://www.oireachtas.ie/documents/bills28/acts/2014/a1114.pdf

[261] Federal Law of the Russian Federation dated December 3, 2008 N 242-FZ "On State Genomic Registration in the Russian Federation" [Unofficial translation] http://www.rg.ru/2008/12/09/genom-registracia-dok.html

[262] Presidência da República Casa Civil Subchefia para Assuntos Jurídicos. LEI No. 12654, DE 28 DE MAIO DE 2012 (in Portuguese). http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12654.htm

[263] COUNCIL DECISION 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. 23rd June 2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:0011:EN:PDF

[264] Ministerio de Justicia, Seguridad y Derechos Humanos. REGISTRO DE HUELLAS DIGITALES GENETICAS. Resolución 415/2004. 21st May 2004. http://infoleg.mecon.gov.ar/infolegInternet/anexos/95000-99999/95342/norma.htm

[265] 22 MARS 1999. - Loi relative à la procédure d'identification par analyse ADN en matière pénale. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1999032252&table_name=loi

[266] BUNDESKRIMINALAMT. Der Datenschutzbeauftragte: DNA-ANALYSE-DATEI. [In German] 29th July 2002. http://www.befreite-dokumente.de/www.befreite-dokumente.de/eingereichte-akten/einrichtungsanordnung-dna/attachment_download/publication_download.pdf
[267] Lei Aprova a criação de uma base de dados de perfis de ADN para fins de identificação civil e criminal. Lei n.º 5/2008, de 12 de Fevereiro. [In Portuguese] http://dre.pt/pdf1sdip/2008/02/03000/0096200968.pdf
[268] Statutes of the Republic of Korea. Act on Use and Protection of DNA Identification Information. Act No. 9944, Jan.25, 2010. Amended by Act No.10258, Apr.15, 2010. Seoul, 2010. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/Korea_law_2010.pdf
[269] Republic of South Africa: Act No. 37 of 2013: Criminal Law (Forensic Procedures). Amendment Act, 2013. Cape Town, 27th January 2014. http://www.justice.gov.za/legislation/acts/2013-037.pdf
[270] Criminal Justice (Forensic Evidence and DNA Database System) Act 2014. Ireland. http://www.oireachtas.ie/documents/bills28/acts/2014/a1114.pdf
[271] UK Home Office (2013) Biennial report 2009 to 2011: National DNA Database. https://www.gov.uk/government/publications/ndnad-biennial-report-2009-to-2011
[272] https://www.fbi.gov/about-us/lab/biometric-analysis/codis/missing-person-comparison-request
[273] 42 U.S. Code § 14136d - DNA identification of missing persons. https://www.law.cornell.edu/uscode/text/42/14136d
[274] Lei Aprova a criação de uma base de dados de perfis de ADN para fins de identificação civil e criminal. Lei n.º 5/2008, de 12 de Fevereiro. [In Portuguese] http://dre.pt/pdf1sdip/2008/02/03000/0096200968.pdf
[275] Lei Aprova a criação de uma base de dados de perfis de ADN para fins de identificação civil e criminal. Lei n.º 5/2008, de 12 de Fevereiro. [In Portuguese] http://dre.pt/pdf1sdip/2008/02/03000/0096200968.pdf
[276] Statutes of the Republic of Korea. Act on Use and Protection of DNA Identification Information. Act No. 9944, Jan.25, 2010. Amended by Act No.10258, Apr.15, 2010. Seoul, 2010. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/Korea_law_2010.pdf
[277] Criminal Justice (Forensic Evidence and DNA Database System) Act 2014. Ireland. http://www.oireachtas.ie/documents/bills28/acts/2014/a1114.pdf
[278] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC
[279]2010 Maryland Code PUBLIC SAFETY TITLE 2 - DEPARTMENT OF STATE POLICE. Subtitle 5 - Statewide DNA Data Base System. Section 2-513 - Annual report. http://law.justia.com/codes/maryland/2010/public-safety/title-2/subtitle-5/2-513/
[280] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC
[281] BUNDESKRIMINALAMT. Der Datenschutzbeauftragte: DNA-ANALYSE-DATEI. [In German] 29th July 2002. http://www.befreite-dokumente.de/www.befreite-dokumente.de/eingereichte-akten/einrichtungsanordnung-dna/attachment_download/publication_download.pdf
[282] BUNDESKRIMINALAMT. Der Datenschutzbeauftragte: DNA-ANALYSE-DATEI. [In German] 29th July 2002. http://www.befreite-dokumente.de/www.befreite-dokumente.de/eingereichte-akten/einrichtungsanordnung-dna/attachment_download/publication_download.pdf
[283] Lei Aprova a criação de uma base de dados de perfis de ADN para fins de identificação civil e criminal. Lei n.º 5/2008, de 12 de Fevereiro. [In Portuguese] http://dre.pt/pdf1sdip/2008/02/03000/0096200968.pdf
[284] DEOXYRIBONUCLEIC ACID (DNA) IDENTIFICATION ACT 2009. Act 699. Malaysia.
[285] German Code of Criminal Procedure in the version published on 7 April 1987 (Federal Law Gazette [Bundesgesetzblatt] Part I p. 1074, 1319), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I p. 410). http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf
[286] BUNDESKRIMINALAMT. Der Datenschutzbeauftragte: DNA-ANALYSE-DATEI. [In German] 29th July 2002. http://www.befreite-dokumente.de/www.befreite-dokumente.de/eingereichte-akten/einrichtungsanordnung-dna/attachment_download/publication_download.pdf

[287] 22 MARS 1999. - Loi relative à la procédure d'identification par analyse ADN en matière pénale. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1999032252&table_name=loi
[288] 42 U.S. Code § 14132 - Index to facilitate law enforcement exchange of DNA identification information. https://www.law.cornell.edu/uscode/text/42/14132
[289] Lei Aprova a criação de uma base de dados de perfis de ADN para fins de identificação civil e criminal. Lei n.º 5/2008, de 12 de Fevereiro. [In Portuguese] http://dre.pt/pdf1sdip/2008/02/03000/0096200968.pdf
[290] 42 U.S. Code § 14132 - Index to facilitate law enforcement exchange of DNA identification information. https://www.law.cornell.edu/uscode/text/42/14132
[291] Rushton S (2010) Familial Searching and Predictive DNA Testing for Forensic Purposes: A Review of Laws and Practices. APPENDIX 1. https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwjYyYu7nvrLAhWDORQKHTvvAdEQFggtMAM&url=http%3A%2F%2Fwww.anzpaa.org.au%2FArticleDocuments%2F220%2Ffamilial-searching-and-predictive-DNA-testing-for-forensic-purposes-a-review-of-law-and-practice.PDF.aspx&usg=AFQjCNFqbYaH39UIAqkl3MHYCq4xaWLsJA
[292] Rushton S (2010) Familial Searching and Predictive DNA Testing for Forensic Purposes: A Review of Laws and Practices. APPENDIX 4. https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwjYyYu7nvrLAhWDORQKHTvvAdEQFggtMAM&url=http%3A%2F%2Fwww.anzpaa.org.au%2FArticleDocuments%2F220%2Ffamilial-searching-and-predictive-DNA-testing-for-forensic-purposes-a-review-of-law-and-practice.PDF.aspx&usg=AFQjCNFqbYaH39UIAqkl3MHYCq4xaWLsJA
[293] 2013 North Carolina General Statutes. Chapter 15A - Criminal Procedure Act. Article 13 - DNA Database and Databank. Section 15A-269 - Request for postconviction DNA testing. http://law.justia.com/codes/north-carolina/2013/chapter-15a/article-13/section-15a-269/
[294] Tennessee Code § 40-30-304 (2015). Post-Conviction DNA Analysis Act of 2001. https://www.lawserver.com/law/state/tennessee/tn-code/tennessee_code_title_40_chapter_30_part_3
[295] Missouri Revised Statutes. Chapter 547. Appeals, New Trials and Exceptions. Section 547.035.1. August 28, 2015. Postconviction DNA testing for persons in the custody of the department--motion, contents--procedure. http://www.moga.mo.gov/mostatutes/stathtml/54700000351.HTML
[296] THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (2012) [ETS No. 108] PROPOSITIONS OF MODERNISATION: Convention for the Protection of Individuals with Regard to the Processing of Personal Data. Council of Europe. T-PD_2012_04_rev4_E. Strasbourg, 18 December 2012. http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282012%2904Rev4_E_Convention%20108%20modernised%20version.pdf
[297] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC
[298] Policy Paper: International DNA exchange policy for the United Kingdom. 23rd October 2015. https://www.gov.uk/government/publications/international-dna-exchange-policy-for-the-united-kingdom
[299] Statement by EU Commissioner Věra Jourová on the finalisation of the EU-US negotiations on the data protection "Umbrella Agreement" (8th September 2015). http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm
[300] Questions and Answers on the EU-US data protection "Umbrella agreement". 8th September 2015. http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm
[301] BUNDESKRIMINALAMT. Der Datenschutzbeauftragte: DNA-ANALYSE-DATEI. [In German] 29th July 2002. http://www.befreite-dokumente.de/www.befreite-dokumente.de/eingereichte-akten/einrichtungsanordnung-dna/attachment_download/publication_download.pdf
[302] Agreement Between the Government of the United States of America and the Government of the Federal Republic of Germany on enhancing cooperation in preventing and combating serious crime. http://www.state.gov/documents/organization/169463.pdf
[303] Statutes of the Republic of Korea. Act on Use and Protection of DNA Identification Information. Act No. 9944, Jan.25, 2010. Amended by Act No.10258, Apr.15, 2010. Seoul, 2010. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/Korea_law_2010.pdf
[304] DEOXYRIBONUCLEIC ACID (DNA) IDENTIFICATION ACT 2009. Act 699. Malaysia.

[305] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26th April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

[306] 42 U.S. Code § 14135e - Privacy protection standards. https://www.law.cornell.edu/uscode/text/42/14135e